

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-236622  
 (43)Date of publication of application : 23.08.2002

---

(51)Int.Cl. G06F 12/14  
 G09C 1/00  
 H04L 9/32

---

(21)Application number : 2001-034969 (71)Applicant : SONY CORP  
 (22)Date of filing : 13.02.2001 (72)Inventor : ASANO TOMOYUKI

---

(54) DEVICE FOR REGENERATING INFORMATION DEVICE FOR RECORDING INFORMATIONMETHOD OF REGENERATING INFORMATIONMETHOD OF RECORDING INFORMATIONRECORDING MEDIUM FOR INFORMATIONAND MEDIUM FOR RECORDING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information recording and regenerating device and a method therefor having a constitution wherein whether legal record content is recorded or not is determined to conduct regenerationin content regeneration.

SOLUTION: A digital signature and a public key certificate are recorded when a data is recorded in an information recording mediumto allow a recorder recorded with a content to be specified. Even when a recording medium containing the data recorded illegally is distributedthe recorder is specified to be eliminated from a system. An information regenerator confirms the reasonability of the signature and the public key certificate when reading out the dataspecifys a content recoring personconfirms no presence of altering in the public key certificate and the digital signatureand regenerates thereafter the data. Use (regeneration) of the record content by the illegal recorder is efficiently eliminated by this constitution.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]Verification processing of an enciphered content record subject's public key certification stored in said recording medium in an information reproducing device which reproduces information from a recording medium is performedSaid

contents recording subject's public key is acquired from a public key certification in which justification was checked. An information reproducing device performing verification processing of a contents recording subject's digital signature and performing decoding processing of enciphered content based on an acquired this public key as a result of this verification on condition that the justification of a signature was checked.

[Claim 2] Said cipher-processing means performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature. The information reproducing device according to claim 1 being the composition of performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 3] Said cipher-processing means performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature. The information reproducing device according to claim 1 being the composition of performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 4] Said information reproducing device holds a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leaf and a leaf key peculiar to each information reproducing device. Said cipher-processing means Decoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said information reproducing device is performed. The information reproducing device according to claim 1 having the composition which acquires data for decryption key generation required for decoding processing of code data stored in said recording medium.

[Claim 5] The information reproducing device according to claim 4 wherein said data for decryption key generation is a medium key peculiar to a common master key or a recording medium in two or more information reproducing devices.

[Claim 6] Have a cipher-processing means to perform encryption processing of contents stored in a recording medium in the Information Storage Division device which records information to a recording medium and this cipher-processing means The Information Storage Division device having the composition which performs processing which generates a digital signature of a record subject of said storing contents matches a public key certification of enciphered content a digital signature and an enciphered content record subject and is stored in a recording medium.

[Claim 7] The Information Storage Division device according to claim 6 having the composition which performs processing which said Information Storage Division device generates storing contents a digital signature and a management table that matched an address of a public key certification and is stored in said recording medium.

[Claim 8]The Information Storage Division device according to claim 6wherein said cipher-processing means is the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature contents of enciphered content stored in said recording mediummatching a generated signature with storing contents and storing it.

[Claim 9]Said cipher-processing means makes applicable to a signature a title key set up corresponding to enciphered content stored in said recording mediumand generation processing of a contents recording subject's digital signature is performedThe Information Storage Division device according to claim 6 being the composition of matching a generated signature with storing contents and storing it.

[Claim 10]Said Information Storage Division device holds a node key peculiar to each node which constitutes hierarchy key tree structure which used several different Information Storage Division devices as a leafand a leaf key peculiar to each Information Storage Division deviceSaid cipher-processing meansDecoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said Information Storage Division device is performed. The Information Storage Division device according to claim 6 having the composition which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.

[Claim 11]The Information Storage Division device according to claim 10wherein said data for cryptographic key generation is a medium key peculiar to a common master key or a recording medium in two or more Information Storage Division devices.

[Claim 12]An information reproduction mode which reproduces information from a recording mediumcomprising:

Public key certification verification steps which perform verification processing of an enciphered content record subject's public key certification stored in said recording medium.

Said contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public keyand a step which performs decoding processing of enciphered content as a result of this signature verification on condition that the justification of a signature was checked.

[Claim 13]Said signature verification steps in said information reproduction modeA step which performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature is includedThe information reproduction mode according to claim 12 performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 14]Said signature verification steps in said information reproduction modeA

step which performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is included. The information reproduction mode according to claim 12 performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[Claim 15] Based on a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leaf further and a leaf key peculiar to each information reproducing device, said information reproduction mode. The information reproduction mode according to claim 12 performing processing which acquires data for decryption key generation required for decoding processing of code data which performed decoding of validation key blocks (EKB) and was stored in said recording medium.

[Claim 16] A cipher-processing step which performs encryption processing of contents stored in a recording medium in an Information Storage Division method which records information to a recording medium. An Information Storage Division method having a step which generates a digital signature of a record subject of said storing contents and enciphered content, a digital signature and a step that matches an enciphered content record subject's public key certification and is stored in a recording medium.

[Claim 17] An Information Storage Division method according to claim 16 performing processing which said Information Storage Division method generates further storing contents, a digital signature and a management table that matched an address of a public key certification and is stored in said recording medium.

[Claim 18] An Information Storage Division method according to claim 16 said Information Storage Division method's making applicable to a signature further contents of enciphered content stored in said recording medium and matching with storing contents a signature which performed and generated generation processing of a contents recording subject's digital signature and storing it.

[Claim 19] Said Information Storage Division method makes applicable to a signature a title key further set up corresponding to enciphered content stored in said recording medium and generation processing of a contents recording subject's digital signature is performed. An Information Storage Division method according to claim 16 matching a generated signature with storing contents and storing it.

[Claim 20] Said Information Storage Division method further. Decoding of validation key blocks (EKB) is performed based on a node key peculiar to each node which constitutes hierarchy key tree structure which used as a leaf a different Information Storage Division device of plurality built in said Information Storage Division device and a leaf key peculiar to each Information Storage Division device. An Information Storage Division method according to claim 16 performing processing which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.

[Claim 21] An information recording medium storing identification data of a record subject who is an information recording medium which stored enciphered

content and recorded this enciphered content said record subject's public key certification and said record subject's digital signature.

[Claim 22] The information recording medium according to claim 21 wherein said information recording medium stores further storing contents a digital signature and a management table that matched an address of a public key certification.

[Claim 23] It is the program storing medium which stored a computer program which makes information reproduction processing which reproduces information from a recording medium perform on computer systems Public key certification verification steps which perform verification processing of a public key certification of an enciphered content record subject by whom said computer program was stored in said recording medium Said contents recording subject's public key is acquired from a public key certification in which justification was checked Signature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public key A program storing medium having a step which performs decoding processing of enciphered content as a result of this signature verification on condition that the justification of a signature was checked.

[Claim 24] It is the program storing medium which stored a computer program which makes the Information Storage Division processing which records information to a recording medium perform on computer systems A cipher-processing step which performs encryption processing of contents which store said computer program in a recording medium A program storing medium having a step which generates a digital signature of a record subject of said storing contents and enciphered contents a digital signature and a step that matches an enciphered content record subject's public key certification and is stored in a recording medium.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention An information reproducing device the Information Storage Division device an information reproduction mode the Information Storage Division method And about an information recording medium and a program storing medium when the Information Storage Division device records data on an information recording medium especially an own digital signature and public key certification are recorded with data When an information reproducing device reads data the justification of the above-mentioned digital signature and a public key certification is checked After checking RIBOKU [ the Information Storage Division device ] it is related with the information reproducing device considered as the composition which reads data the Information Storage Division device an information reproduction mode the Information Storage Division method an information recording medium and a program storing medium.

[0002]

[Description of the Prior Art] In recent years the recorder and recording medium which record information in digital one are spreading with progress of digital signal processing technology and development. According to such a digital recording apparatus and a recording medium record and reproduction can be repeated without degrading a picture and a sound for example. Thus since the digital data can carry out repeat execution of the copy repeatedly with image quality or tone quality maintained when the recording medium with which the copy was performed illegally will circulate in a commercial scene profitssuch as an owner of a copyright of various contentssuch as music and a movie or a just dealership person will be injured. In these days in order to prevent the unjust copy of such digital data various structure (system) for preventing an illegal copy is introduced into the digital recording apparatus and the recording medium.

[0003] For example in MD (mini disc) (MD is trademark) device SCMS (Serial Copy Management System) is adopted as a method of preventing an illegal copy. In [ SCMS outputs a SCMS signal to the data reproduction side from a digital interface (DIF) with audio information and ] the Data Recording Sub-Division side It is a system which prevents an illegal copy by controlling record of the audio information from the reproduction side based on the SCMS signal from the reproduction side.

[0004] A SCMS signal specifically. [ whether audio information is data of copy free (copy free) in which a copy is permitted any number of times and ] It is a signal showing whether it is data in which the copy is allowed only once (copy once allowed) or it is data in which the copy is forbidden (copy prohibited). If audio information is received from DIF to the Data Recording Sub-Division side the SCMS signal transmitted with the audio information will be detected. And when the SCMS signal serves as copy free (copy free) audio information is recorded on a mini disc with a SCMS signal. When the SCMS signal is permitted (copy once allowed) once about the copy a SCMS signal is changed into copy prohibition (copy prohibited) and it records on a mini disc with audio information. Audio information is not recorded when the SCMS signal serves as copy prohibition (copy prohibited). By performing control which uses such SCMS the audio information which has copyright prevents being copied illegally by SCMS with a mini disc device.

[0005] However since it is a premise that the apparatus itself which records data has the composition which controls record of the audio information from the reproduction side based on a SCMS signal as mentioned above as for SCMS When a mini disc device without the composition which performs control of SCMS is manufactured it becomes difficult to cope with it. Then for example with the DVD player it has the composition of preventing the illegal copy of data which has copyright by adopting a contents scramble system.

[0006] In a contents scramble system to DVD-ROM (Read Only Memory). A video data audio information etc. are enciphered and recorded and the key (decode key) used for decoding the enciphered data is given to the licensed DVD player. It is

licensed to the DVD player designed follow predetermined regulation of not copying illegally of operation. Therefore in the licensed DVD player an image and a sound are renewable from DVD-ROM by decoding the encryption data recorded on DVD-ROM using the given key.

[0007] On the other hand since the DVD player which has not been licensed does not have a key for decoding the enciphered data it cannot decode the encryption data recorded on DVD-ROM. Thus in contents scramble system composition the DVD player which does not fulfill the conditions demanded at the time of a license can reproduce DVD-ROM which recorded digital data and an illegal copy is prevented.

[0008] However the contents scramble system adopted with DVD-ROM is aimed at the recording medium (suitably henceforth ROM media) which cannot write in the data by a user.

It is not taken into consideration about application to the recording medium (suitably henceforth RAM media) which can write in the data by a user.

[0009] That is even if the data recorded on ROM media was enciphered when the enciphered data is all copied to RAM media as it was what is called a refreshable pirate edition will be able to be created with the licensed just device.

[0010] Then in previous patent application and JPH11-224461A (Tokuganhei10-25310) these people record the information (it is hereafter described as medium identification information) for identifying each recording medium on a recording medium with other data and on condition that it is the device which received the license of this medium identification information it carries out. Only when the condition was fulfilled the composition whose access to the medium identification information of a recording medium is attained was proposed.

[0011] The data on a recording medium is enciphered in this method by the secret key (master key) obtained by receiving medium identification information and a license. Meaningful data cannot be obtained even if the device which has not been licensed reads this enciphered data. When a device is licensed the operation is specified so that an unjust duplicate (illegal copy) may not be made.

[0012] Since the device which has not been licensed cannot access medium identification information and medium identification information serves as an individual value for each medium of every. Even if the device which has not been licensed reproduces all the enciphered data that is recorded on the recording medium to a new recording medium since the data recorded on the recording medium created by making it such cannot be correctly decoded in the licensed device as well as the device which has not been licensed an illegal copy will be prevented substantially.

[0013] By the way as for the master key stored in the licensed device in the above-mentioned composition it is common in a complete aircraft machine that it is common. Thus it is because it is conditions required in order that storing a common master key to two or more apparatus may make refreshable the medium recorded by one apparatus by other apparatus (interoperability is secured).

[0014] However, in this method, when an aggressor succeeds in the attack of one apparatus and takes out a master key, the data currently enciphered and recorded in all the systems can be decoded and the whole system collapses. In order to prevent this, when a certain apparatus was attacked and the master key exposed is revealed, it is necessary to give the master key which updated the master key to a new thing and was newly updated by complete aircraft machines other than the apparatus which yielded to the attack. Although the peculiar key (debye skiing) is given to each apparatus as a method simple No. 1 which realizes this composition, the value which enciphered a new master key on each debye skis is prepared and the method transmitted to apparatus via a recording medium can be considered. There is a problem that the total amount of messages which should be transmitted in proportion to the number of apparatus increases.

[0015] As a composition which solves the above-mentioned problem, these people Via a recording medium or a communication line using the key distribution method of composition of having arranged each Information Storage Division playback equipment to each wooden leaf (leaf) for n minutes. When a key (a master key or a medium key) required for the record to the recording medium of contents data or the reproduction from a recording medium is distributed and each device is made to perform record of contents data and reproduction using this. The just (to device which the secret has not exposed) composition which receives and can transmit a master key or a medium key in the small amount of messages is proposed previously and patent application (Japanese Patent Application No. 2000-105328) has already been carried out. The key which is specifically needed in order to generate a key required for the record to a recording medium or the reproduction from a recording medium. For example, the node key assigned to the node which constitutes each wooden leaf (leaf) for n minutes is set up as an updating node key. The leaf key in which only just apparatus has an updating node key and validation key blocks (EKB) including the information which carried out encryption processing in the mode which can decode by a node key are distributed to each Information Storage Division playback equipment. It is the composition which made acquirable the key which each device needs for record or the reproduction from a recording medium by the EKB decoding processing of each Information Storage Division playback equipment which received validation key blocks (EKB).

[0016]

[Problem(s) to be Solved by the Invention] In the above-mentioned composition, although it is possible to eliminate from a system the device which the secret exposed, it is necessary to specify whether for the purpose it was exposed of the secret of which device. For example, the clone device which carries the secret of which a certain device was robbed is made and if it can specify having been sold in the black market, the device with which the secret was stolen will be specified and it will be eliminated from a system.

[0017] By the way, considering the attack on a system, a clone device is made as mentioned above and it does not appear on the market. The act of selling the recording medium of converting a certain Information Storage Division device for



example recording the data which should be enciphered essentially and should be recorded by a plaintext which made perform unjust record and was made as a result and containing the data recorded unjustly can be considered. In this case if the device which recorded data on that recording medium unjustly can be specified it is possible by the above-mentioned method to distribute so that it may be eliminated from a system and new contents data may not be made to decode with that device.

[0018] This invention solves an above-mentioned problem.

The purpose records an own digital signature and public key certification with data when the Information Storage Division device records data on an information recording medium. When an information reproducing device reads data after checking the justification of the above-mentioned digital signature and a public key certification by having composition which reads data it is providing the system which makes reproduction possible on condition that contents recording's is performed justly.

[0019]

[Means for Solving the Problem] In an information reproducing device with which the 1st side of this invention reproduces information from a recording medium. Perform verification processing of an enciphered content record subject's public key certification stored in said recording medium and said contents recording subject's public key is acquired from a public key certification in which justification was checked. Based on an acquired this public key verification processing of a contents recording subject's digital signature is performed and it is in an information reproducing device performing decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this verification.

[0020] An information reproducing device of this invention sets like 1 operative condition and said cipher-processing means. It is characterized by being the composition of performing verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature and performing decoding processing of enciphered content as a result of this verification on condition that the justification of a signature was checked.

[0021] An information reproducing device of this invention sets like 1 operative condition and said cipher-processing means. Verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is performed. It is characterized by being the composition of performing decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this verification.

[0022] An information reproducing device of this invention sets like 1 operative condition and said information reproducing device. Hold a node key peculiar to each node which constitutes hierarchy key tree structure which used several different

information reproducing devices as a leaf and a leaf key peculiar to each information reproducing device and said cipher-processing means decoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said information reproducing device is performed. It has the composition which acquires data for decryption key generation required for decoding processing of code data stored in said recording medium.

[0023] An information reproducing device of this invention sets like 1 operative condition and said data for decryption key generation is characterized by being a medium key peculiar to a common master key or a recording medium in two or more information reproducing devices.

[0024] In the Information Storage Division device with which the 2nd side of this invention records information to a recording medium, have a cipher-processing means to perform encryption processing of contents stored in a recording medium and this cipher-processing means a digital signature of a record subject of said storing contents is generated and it is in enciphered content, a digital signature and the Information Storage Division device having the composition which performs processing which matches an enciphered content record subject's public key certification and is stored in a recording medium.

[0025] The Information Storage Division device of this invention sets like 1 operative condition, said Information Storage Division device generates storing contents, a digital signature and a management table that matched an address of a public key certification and it has the composition which performs processing stored in said recording medium.

[0026] The Information Storage Division device of this invention sets like 1 operative condition and said cipher-processing means it is characterized by being the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature contents of enciphered content stored in said recording medium, matching a generated signature with storing contents and storing it.

[0027] The Information Storage Division device of this invention sets like 1 operative condition and said cipher-processing means it is characterized by being the composition of performing generation processing of a contents recording subject's digital signature by making applicable to a signature a title key set up corresponding to enciphered content stored in said recording medium, matching a generated signature with storing contents and storing it.

[0028] The Information Storage Division device of this invention sets like 1 operative condition and said Information Storage Division device holds a node key peculiar to each node which constitutes hierarchy key tree structure which used several different Information Storage Division devices as a leaf and a leaf key peculiar to each Information Storage Division device and said cipher-processing means decoding of validation key blocks (EKB) which consist of encryption processed data of a higher rank key by a low rank key on a path of a key tree based on a key built in said Information Storage Division device is performed. It

has the composition which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium.

[0029]The Information Storage Division device of this invention sets like 1 operative condition and said data for cryptographic key generation is characterized by being a medium key peculiar to a common master key or a recording medium in two or more Information Storage Division devices.

[0030]In an information reproduction mode with which the 3rd side of this invention reproduces information from a recording mediumPublic key certification verification steps which perform verification processing of an enciphered content record subject's public key certification stored in said recording mediumSaid contents recording subject's public key is acquired from a public key certification in which justification was checkedSignature verification steps which perform verification processing of a contents recording subject's digital signature based on an acquired this public keyIt is in an information reproduction mode having a step which performs decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this signature verification.

[0031]Said signature verification steps [ in / an information reproduction mode of this invention sets like 1 operative condition and / said information reproduction mode ]A step which performs verification processing of a contents recording subject's digital signature generated considering contents of enciphered content stored in said recording medium as a candidate for a signature is includedAs a result of this verification on condition that the justification of a signature was checked decoding processing of enciphered content is performed.

[0032]Said signature verification steps [ in / an information reproduction mode of this invention sets like 1 operative condition and / said information reproduction mode ]A step which performs verification processing of a contents recording subject's digital signature generated considering a title key set up corresponding to enciphered content stored in said recording medium as a candidate for a signature is includedAs a result of this verification on condition that the justification of a signature was checked decoding processing of enciphered content is performed.

[0033]An information reproduction mode of this invention sets like 1 operative condition and said information reproduction modeBased on a node key peculiar to each node which constitutes hierarchy key tree structure which used several different information reproducing devices as a leaf and a leaf key peculiar to each information reproducing deviceProcessing which acquires data for decryption key generation required for decoding processing of code data which performed decoding of validation key blocks (EKB) and was stored in said recording medium is performed.

[0034]In an Information Storage Division method that the 4th side of this invention records information to a recording mediumA cipher-processing step which performs encryption processing of contents stored in a recording mediumIt is in an Information Storage Division method having a step which generates a digital signature of a record subject of said storing contents and enciphered contents

digital signature and a step that matches an enciphered content record subject's public key certification and is stored in a recording medium.

[0035] An Information Storage Division method of this invention sets like 1 operative condition said Information Storage Division method generates further storing contents a digital signature and a management table that matched an address of a public key certification and processing stored in said recording medium is performed.

[0036] An Information Storage Division method of this invention sets like 1 operative condition and said Information Storage Division method Generation processing of a contents recording subject's digital signature is performed by making applicable to a signature contents of enciphered content stored in said recording medium and a generated signature is matched with storing contents and stored.

[0037] An Information Storage Division method of this invention sets like 1 operative condition and said Information Storage Division method Generation processing of a contents recording subject's digital signature is performed by making applicable to a signature a title key set up corresponding to enciphered content stored in said recording medium and a generated signature is matched with storing contents and stored.

[0038] An Information Storage Division method of this invention sets like 1 operative condition and said Information Storage Division method Furthermore Decoding of validation key blocks (EKB) is performed based on a node key peculiar to each node which constitutes hierarchy key tree structure which used as a leaf a different Information Storage Division device of plurality built in said Information Storage Division device and a leaf key peculiar to each Information Storage Division device. Processing which acquires data for cryptographic key generation required for data encryption processing stored in said recording medium is performed.

[0039] The 5th side of this invention is the information recording medium which stored enciphered content and is in an information recording medium storing identification data of a record subject who recorded this enciphered contents said record subject's public key certification and said record subject's digital signature.

[0040] An information recording medium of this invention set like 1 operative condition and said information recording medium stored further storing contents a digital signature and a management table that matched an address of a public key certification.

[0041] The 6th side of this invention is the program storing medium which stored a computer program which makes information reproduction processing which reproduces information from a recording medium perform on computer systems Public key certification verification steps which perform verification processing of a public key certification of an enciphered content record subject by whom said computer program was stored in said recording medium Said contents recording subject's public key is acquired from a public key certification in which justification was checked Signature verification steps which perform verification

processing of a contents recording subject's digital signature based on an acquired this public key. It is in a program storing medium having a step which performs decoding processing of enciphered content on condition that the justification of a signature was checked as a result of this signature verification.

[0042] The 7th side of this invention is the program storing medium which stored a computer program which makes the Information Storage Division processing which records information to a recording medium perform on computer systems. A cipher-processing step which performs encryption processing of contents which store said computer program in a recording medium. It is in a program storing medium having a step which generates a digital signature of a record subject of said storing contents and enciphered content, a digital signature and a step that matches an enciphered content record subject's public key certification and is stored in a recording medium.

[0043]

[Function] In this invention, when the Information Storage Division device recorded data on an information recording medium, an own digital signature and public key certification were recorded with data. Since he is trying to also certainly record with data proof which recorder recorded by this when recording information. Since it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulated, exclusion from a system can be performed.

[0044] When an information reproducing device reads data after checking the justification of the above-mentioned digital signature and a public key certification, it had composition which reads data. By this, the inaccurate recorder is delivering the powerless thing an attack which does not record a digital signature to inaccurate record data. That is, it is because just playback equipment will not reproduce the data if there is no effective digital signature to the recorded data.

[0045]

[Embodiment of the Invention] [System configuration] Drawing 1 is a block diagram showing one working example composition of the recording and reproducing device 100 which applied this invention. The recording and reproducing device 100 Input-and-output I/F. 120 (Interface) MPEG (Moving.) Input-and-output I/F (Interface) 140 [ provided with the Picture Experts Group codec 130 A/D and D/A converter 141 ] the cipher-processing means 150 ROM (Read Only Memory) 160 CPU (Central.) Processing Unit 170 the memory 180 and the recording-medium interface (I/F) 190 of the recording medium 200 -- it has the transport stream processing means (TS processing means) 300 further and these are mutually connected by bus 110.

[0046] Input-and-output I/F 120 receives the digital signal on the bus 110 and outputs it outside while it receives the digital signal which constitutes various contents supplied from the outside such as a picture, a sound and a program and outputs it on the bus 110. The MPEG codec 130 carries out MPEG encoding of the digital signal supplied from input-and-output I/F 140 and outputs it on the bus 110 while it carries out MPEG decoding of the data which is supplied via the bus 110 and by which MPEG coding was carried out and outputs it to input-and-output I/F 140. Input-and-output I/F 140 builds in A/D and D/A converter 141. It is

input-and-output I/F140 receiving the analog signal as contents supplied from the outside and carrying out A/D (Analog Digital) conversion by A/D and D/A converter 141. As a digital signal while outputting to the MPEG codec 130, the digital signal from the MPEG codec 130 is outputted outside as an analog signal by carrying out D/A (Digital Analog) conversion by A/D and D/A converter 141.

[0047] For example, the cipher-processing means 150 comprises LSI (Large Scale Integrated Circuit) of one chip which enciphers or decodes the digital signal as contents supplied via the bus 110 and has the composition outputted on the bus 110. Not only 1 chip LSI but the thing which the composition which combined various kinds of software or hardware realizes is possible for the cipher-processing means 150. The latter part explains the composition as a processing means by a software configuration.

[0048] ROM160 has memorized the leaf key which is peculiar to debye skiing and the node key which are two or more recording and reproducing devices or debye skiing shared in two or more groups for every recording and reproducing device for every group of two or more peculiar to recording and reproducing devices for example. The secret key of a public-key-encryption system peculiar to a recording and reproducing device and the public key of the public key certification and the further reliable center are memorized.

[0049] Here, the center (certificate authority) which a public key certification stores the certificate user's for example ID of a recording and reproducing device and a user public key as shown in drawing 2 and can trust other data as a message is the data which gave the digital signature. Verification processing of the digital signature of a center can be performed using the public key of an acquired center beforehand, the justification of a public key certification can be checked and the stored public key can be taken out and used.

[0050] CPU170 is executing the program memorized by the memory 180 and controls the MPEG codec 130 and cipher-processing means 150. The memory 180 is nonvolatile memory and memorizes required data on the program which CPU170 executes and operation of CPU170 for example. While the recording-medium interface 190 reads digital data from the recording medium 200 (reproducing) and outputs it on the bus 110 by driving the recording medium 200 in which record reproduction is possible for digital data. The digital data supplied via the bus 110 is supplied to the recording medium 200 and is made to record. It is good also as composition which memorizes a program to ROM160 and memorizes debye skiing etc. in the memory 180.

[0051] The recording medium 200 is a medium which can memorize digital data such as semiconductor memory such as optical disc such as DVD and CD, a magnetic optical disc, a magnetic disk, a magnetic tape or RAM for example. According to this embodiment, suppose that it is removable composition to the recording-medium interface 190.

However, the recording medium 200 is good also as composition built in the recording and reproducing device 100.

[0052] Although the transport stream processing means (TS processing means)

300 is explained in detail using figures in the latter part. For example, the transport packet corresponding to a specific program (contents) is taken out from the transport stream which two or more TV programs (contents) multiplexed. Data processing for storing the appearance timing information of the taken-out transport stream in the recording medium 200 with each packet and appearance timing-control processing at the time of the regeneration from the recording medium 200 are performed.

[0053] ATS (Arrival Time Stamp: mail arrival time stamp) as appearance timing information of each transport packet is set to the transport stream.

It is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systems and at the time of reproduction of a transport stream.

Appearance timing is controlled by ATS added to each transport packet.

The transport stream processing means (TS processing means) 300 performs these control. For example, in recording a transport packet on a recording medium, record as a source packet which packed the interval of each packet but. By saving the appearance timing of each transport packet collectively at a recording medium, it becomes possible to control the output timing of each packet at the time of reproduction. The transport stream processing means (TS processing means) 300 adds and records ATS (Arrival Time Stamp: mail arrival time stamp) showing the input timing of each transport packet at the time of Data Recording Sub-Division to the recording media 200 such as DVD.

[0054] The data processed in the processing system of this invention is not restricted to the format data according to a transport stream. Therefore, when performing processing about data other than a transport stream, it is not necessarily necessary for TS processing means shown in drawing 1.

[0055] [The Data Recording Sub-Division processing and data reproduction processing] Next, the Data Recording Sub-Division processing and the data reproduction processing from a recording medium to the recording medium in the recording and reproducing device of drawing 1 are explained with reference to the flow chart of drawing 3 and drawing 4. When recording the contents of the digital signal from the outside on the recording medium 200, recording processing according to the flow chart of drawing 3 (A) is performed. Namely, the contents (digital contents) of a digital signal. For example, via IEEE (Institute of Electrical and Electronics Engineers) 1394 serial bus etc. If input-and-output I/F 120 is supplied in Step S11, input-and-output I/F 120 will receive the digital contents supplied and will output them to TS processing means 300 or the cipher-processing means 150 via the bus 110.

[0056] When received data need transport stream processing, transport stream processing is performed in TS processing means 300. In Step S12, TS processing means 300 generates the block data which added ATS to each transport packet which constitutes a transport stream and outputs it to the cipher-processing means 150 via the bus 110. This processing is explained still in detail in the latter part.

[0057]In Step S13the cipher-processing means 150 performs encryption processing to the digital contents which receivedand outputs the enciphered content obtained as a result to recording-medium I/F190 via the bus 110. Enciphered content is recorded on the recording medium 200 via recording-medium I/F190 (S14)and ends recording processing.

[0058]Between [ connected via the IEEE1394 serial bus ] devicesBy five companies which include Sony Corp. which is this Applicant as a standard for protecting digital contents when transmitting digital contents. Although 5CDTCP (Five Company Digital Transmission Content Protection) (suitably henceforth DTCP) is definedWhen the digital contents which are not free as for a copy are transmitted between devices in this DTCPIn [ attest mutually whether in advance of data communicationthe transmitting side and a receiver can deal with the copy control information for controlling a copy correctlyand ] after that and the transmitting sideDigital contents are enciphered and transmitted and the enciphered digital contents (enciphered content) are decoded in a receiver.

[0059]In the data transmission and reception based on a standard to this DTCPInput-and-output I/F120 of a data receiving side is Step S11it receives enciphered content via an IEEE1394 serial busdecodes the enciphered content to DTCP based on a standardand outputs it to the cipher-processing means 150 after that as contents of a plaintext.

[0060]The key which carries out a temporal change is generated and encryption of the digital contents by DTCP is performed using the key. The enciphered digital contents are transmitted in IEEE1394 serial bus tops including the key used for the encryptionand decode the enciphered digital contents in a receiver using the key contained there.

[0061]According to DTCPthe initial value of a key and the flag showing the changing timing of a key used for encryption of digital contents are correctly included in enciphered content. And at a receiverby changing too the initial value of the key contained in the enciphered content in the timing of the flag contained in the enciphered contentthe key used for encryption is generated and enciphered content is decoded. Howeverif the key for performing the decoding to enciphered content is containedeven if it will think that it is equivalentin order not to interferebelowit shall think such here. In the Web page specified by URL (Uniform Resource Locator) of <http://www.dtcp.com> about DTCP herefor exampleAcquisition of an informational version (Informational Version) is possible.

[0062]Nextthe contents of the analog signal from the outside are explained about the processing in the case of recording on the recording medium 200 according to the flow chart of drawing 3 (B). When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S21the analog content is receivedan A/D conversion is carried out by A/D and D/A converter 141 which are followed and built in Step S22and it is considered as the contents (digital contents) of a digital signal.

[0063]These digital contents are supplied to the MPEG codec 130and in Step S23coding processing by MPEG encodingi.e.MPEG compressionis performedand



they are supplied to the cipher-processing means 150 via the bus 110.

[0064] Hereafter in Step S24, S25 and S26 processing in Step S12 of drawing 3 (A), S13 and S14 and same processing are performed. That is, if required, ATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means 150 will be performed. The enciphered content obtained as a result is recorded on the recording medium 200 and recording processing is ended.

[0065] Next, the contents recorded on the recording medium 200 are reproduced and the processing outputted as digital contents or analog content is explained according to the flow of drawing 4. Processing outputted outside as digital contents is performed as regeneration according to the flow chart of drawing 4 (A). That is, first in Step S31, the enciphered content recorded on the recording medium 200 is read by recording-medium I/F190 and it is outputted to the cipher-processing means 150 via the bus 110.

[0066] In the cipher-processing means 150, decoding processing of the enciphered content supplied from recording-medium I/F190 is carried out in Step S32 and when data is a transport stream, Decode data is outputted to TS processing means 300 via the bus 110 and when TS processing is unnecessary, input-and-output I/F120 is supplied.

[0067] In Step S43, TS processing means 300 judges output timing from ATS of each transport packet which constitutes a transport stream, performs control according to ATS and supplies it to input-and-output I/F120 via the bus 110. Input-and-output I/F120 outputs the digital contents from TS processing means 300 outside and ends regeneration. The decoding processing of the digital contents in processing of TS processing means 300 and the cipher-processing means 150 is mentioned later.

[0068] Data is supplied to input-and-output I/F120 and in Step S34, input-and-output I/F120 outputs digital contents outside and ends regeneration.

[0069] Input-and-output I/F120 in Step S34, based on the standard of DTCP, when outputting digital contents via an IEEE1394 serial bus as mentioned above, attests mutually between a partner's devices and enciphers and transmits digital contents after that.

[0070] When reproducing the contents recorded on the recording medium 200 and outputting outside as analog content, regeneration according to the flow chart of drawing 4 (B) is performed.

[0071] Namely, in Step S41, S42 and S43, the respectively same processing as the case in Step S31 of drawing 4 (A), S32 and S33 is performed and by this, the decoded digital contents which were obtained in the cipher-processing means 150 are supplied to the MPEG codec 130 via the bus 110.

[0072] In the MPEG codec 130, in Step S44, MPEG decoding, i.e., elongation processing, is executed and digital contents are supplied to input-and-output I/F140. In Step S44, D/A conversion (S45) of the digital contents by which MPEG decoding was carried out by the MPEG codec 130 is carried out by A/D and D/A converter 141 to build in and input-and-output I/F140 makes them analog content.

And it progresses to Step S46 and input-and-output I/F140 outputs the analog content outside and ends regeneration.

[0073][Transport stream] Next the data format on the recording medium in the case of processing transport stream data is explained using drawing 5. The minimum unit of reading and writing of the data on a recording medium is called by the name of the block (block). 1 block has  $192 \times X$  (X) byte's (for example  $X = 32$ ) size.

[0074] For example ATS is added to TS (transport stream) packet (188 bytes) of MPEG 2 and as 192 bytes  $X$  of them are collected and it is considered as 1-block data. ATS is data in which 24 thru/ or 32-bit mail arrival time is shown and is the abbreviation for Arrival Time Stamp (mail arrival time stamp). ATS is constituted as data with the random nature according to the mail arrival time of each packet.  $X$  individual record of the TS (transport stream) packet which added ATS to one block (sector) of a recording medium is carried out. In the composition of this invention the block key which enciphers the data of the block (sector) using ATS added to the 1st TS packet of each block which constitutes a transport stream is generated.

[0075] By generating the block key for encryption using ATS with random nature a different inherent key for every block is generated. Encryption processing for every block is performed using the generated block inherent key. By having composition which generates a block key using ATS the field on the recording medium for storing the enciphering key for every block becomes unnecessary and a main data area becomes usable effectively. It becomes unnecessary to access any data other than a main data division at the time of record of data and reproduction and processing becomes efficient.

[0076] Block seed (Block Seed) shown in drawing 5 is the additional information containing ATS. The composition which copy limit information (CCI: Copy Control Information) also adds as further shown not only in ATS but in the figure middle is possible for block seed. In this case it can have composition which generates a block key using ATS and CCI.

[0077] In the composition of this invention when it stores data on recording media such as DVD the data of most contents is enciphered but. As shown in the bottom of drawing 5  $m$  (for example  $m = 8$  or  $16$ ) byte of the head of a block is recorded with a plaintext (Unencrypted data) without being enciphered and the remaining data ( $m+1$  byte or subsequent ones) is enciphered. This is for restrictions to occur in cipher-processing data length (Encrypted data) since cipher processing is processing as an 8-byte unit. If cipher processing can carry out for example not per 8-byte unit but per byte all portions other than block seed may be enciphered as  $m = 4$ .

[0078] [Processing in TS processing means] Here the function of ATS is explained in detail. ATS is a mail arrival time stamp added since the appearance timing of each transport packet in an input transport stream is saved as explained also in advance.

[0079] Namely when one or some TV programs (contents) are taken out of the

transport stream which two or more TV programs (contents) multiplexed for example. The transport packet which constitutes the taken-out transport stream appears at an irregular interval (refer to drawing 7 (a)). A transport stream has a meaning important for the appearance timing of each transport packet. It is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systems (ISO/IEC 13818-1).

[0080] Appearance timing is controlled by ATS added to each transport packet at the time of reproduction of a transport stream. Therefore in recording a transport packet on a recording medium. When it is necessary to save the input timing of a transport packet and a transport packet is recorded on recording media such as DVD, ATS showing the input timing of each transport packet is added and recorded.

[0081] The block diagram explaining the processing which performs the transport stream inputted via a digital interface in TS processing means 300 when recording on the storage medium which are recording media such as DVD is shown in drawing 6. From the terminal 600a a transport stream is inputted as digital data such as digital broadcasting. In drawing 1 a transport stream is inputted from the terminal 600 via input-and-output I/F 140 and the MPEG codec 130 via input-and-output I/F 120.

[0082] A transport stream is inputted into the bit stream purser (parser) 602. The bit stream purser 602 detects an PCR (Program Clock Reference) packet out of an input transport stream. Here an PCR packet is a packet by which PCR specified with MPEG 2 systems is coded. The PCR packet is coded with the time interval of less than 100 msec. PCR expresses with the accuracy of 27 MHz the time when a transport packet reaches a receiver.

[0083] And PCR of a transport stream is made to carry out lock (Lock) of the 27 MHz clocks which a record reproducer has in 27MHz PLL 603. The time stamp generation circuit 604 generates the time stamp based on the counted value of the clock of 27 MHz clocks. And the block seed (Block seed) additional circuit 605 is added to the transport packet by setting a time stamp in case the 1st byte of a transport packet is inputted into the smoothing buffer 606 to ATS.

[0084] The transport packet to which ATS was added. It passes along the smoothing buffer 606 and after cipher processing which it is outputted to the cipher-processing means 150 and is explained in the latter part from the terminal 607 is performed. It is recorded on the recording medium 200 which is a storage medium via recording-medium I/F 210 (drawing 1).

[0085] Drawing 7 shows the example of processing in case an input transport stream is recorded on a recording medium. Drawing 7 (a) shows the input of the transport packet which constitutes a certain specific program (contents). A horizontal axis is a time-axis which shows the time on a stream here. In this example the input of a transport packet appears to irregular timing as shown in drawing 7 (a).

[0086] Drawing 7 (b) shows the output of the block seed (Block Seed) additional circuit 605. The block seed (Block Seed) additional circuit 605 adds the block seed

(Block Seed) containing ATS which shows the time on the stream of the packet for every transport packet and outputs a source packet. Drawing 7 (c) shows the source packet recorded on the recording medium. As shown in drawing 7 (c) a source packet packs an interval and is recorded on a recording medium. Thus the record section of a recording medium can be effectively used by packing and recording an interval.

[0087] Drawing 8 shows the processing constitution block diagram of TS processing means 300 in the case of reproducing the transport stream recorded on the recording medium 200. The transport packet with ATS decoded in a cipher-processing means to explain in the latter part is inputted into the block seed (Block seed) separation circuits 801 and ATS and a transport packet are separated from the terminal 800. The timing generating circuit 804 calculates the time based on the clock counter value of 27 MHz clocks 805 which a regenerator has.

[0088] Very first ATS is set to the timing generating circuit 804 as an initial value at the time of a reproductive start. The comparator 803 compares the present time inputted from ATS and the timing generating circuit 804. And when time for the timing generating circuit 804 to occur and ATS become equal the output controlling circuit 802 outputs the transport packet to the MPEG codec 130 or digital-input/output I/F120.

[0089] Drawing 9 carries out MPEG encoding of the input AV signal in the MPEG codec 130 of the record reproducer 100 and shows the composition which codes a transport stream in TS processing means 300 further. Therefore drawing 9 is a block diagram showing both the processing constitution of the MPEG codec 130 and TS processing means 300 in drawing 1 collectively. The video signal is inputted from the terminal 901 and it is inputted into MPEG video encoder 902.

[0090] MPEG video encoder 902 codes an input video signal to an MPEG video stream and outputs it to the buffer video stream buffer 903. MPEG video encoder 902 outputs the access unit information about an MPEG video stream to the multiplexing scheduler 908. The access unit of a video stream is a picture and access unit information is a picture type of each picture and an encoding bit amount and a decoding time stamp. Here a picture type is the information on I/P/B picture (picture). A decoding time stamp is information specified with MPEG 2 systems.

[0091] The audio signal is inputted from the terminal 904 and it is inputted into MPEG audio encoder 905. MPEG audio encoder 905 codes an input audio signal to an MPEG audio stream and outputs it to the buffer 906. MPEG audio encoder 905 outputs the access unit information about an MPEG audio stream to the multiplexing scheduler 908. The access unit of an audio stream is an audio frame and access unit information is an encoding bit amount of each audio frame and a decoding time stamp.

[0092] The access unit information of video and an audio is inputted into the multiplexing scheduler 908. The multiplexing scheduler 908 controls the method of coding a video stream and an audio stream to a transport packet based on access unit information. As the multiplexing scheduler 908 has a clock which generates the reference time of 27-MHz accuracy in an inside and fills T-STD which is the

virtual decoder model specified by MPEG 2it determines the packet encoding control information of a transport packet. Packet encoding control information is the kind of stream and the length of a stream which are packet-ized.

[0093]When packet encoding control information is a video packetit is on the a sidethe video data of payload-data length directed by packet encoding control information is read from the video stream buffer 903and the switch 976 is inputted into the transport packet coding equipment 909.

[0094]When packet encoding control information is an audio packetit is on the b sidethe audio information of payload-data length directed from the audio stream buffer 906 is readand the switch 976 is inputted into the transport packet coding equipment 909.

[0095]When packet encoding control information is an PCR packetthe transport packet coding equipment 909 incorporates PCR inputted from the multiplexing scheduler 908and outputs an PCR packet. Nothing is inputted into the transport packet coding equipment 909 when directing that packet encoding control information does not code a packet.

[0096]The transport packet coding equipment 909 does not output a transport packetwhen directing that packet encoding control information does not code a packet. When othera transport packet is generated and outputted based on packet encoding control information. Thereforethe transport packet coding equipment 909 outputs a transport packet intermittently. The arrival (Arrival) time stamp (time stamp) calculating means 910 calculates ATS which shows the time when the 1st byte of a transport packet reaches a receiver based on PCR inputted from the multiplexing scheduler 908.

[0097]Since PCR inputted from the multiplexing scheduler 908 shows the arrival time to the 10th byte of receiver of the transport packet specified by MPEG 2the value of ATS serves as time when the byte 10 bytes before the time of PCR arrives.

[0098]The block seed (Block Seed) additional circuit 911 adds ATS to the transport packet outputted from the transport packet coding equipment 909. The transport packet with ATS outputted from the block seed (Block seed) additional circuit 911It passes along the smoothing buffer 912a cipher-processing means 150 HE input is carried outand it is stored in the recording medium 200 which is a storage medium after cipher processing explained in the latter part is performed.

[0099]Before being enciphered by the cipher-processing means 150the transport packet with ATS stored in the recording medium 200 is inputted where an interval is packedas shown in drawing 7 (c)and it is stored in the recording medium 200 after that. Even if a transport packet packs an interval and is recordedthe input time to the receiver of the transport packet is controllable by referring to ATS.

[0100]By the waythe size of ATS was not necessarily decided as 32 bitsand 24 bits thru/or 31 bits of it may be sufficient. The cycle around which the time counter of ATS goes becomes longso that the bit length of ATS is long. For examplewhen ATS is a binary counter of 27-MHz accuracytime for ATS of 24-bit length to go around is about 0.6 second. This time interval is size sufficient in a

general transport stream. It is because the packet interval of the transport stream is decided to be a maximum of 0.1 second by regulation of MPEG 2.

However sufficient margin is seen and it is good as for more than 24-bit in ATS.

[0101] Thus when bit length of ATS is made into various lengths some composition is attained as composition of the block seed who is attached data of block data.

Block seed's example of composition is shown in drawing 10. Example 1 of drawing 10 is an example which uses ATS by 32 bits. Example 2 of drawing 10 is an example which makes ATS 30 bits and uses copy control information (CCI) by 2 bits. Copy control information is information showing the state of copy-of-data control where it was added.

SCMS: Serial Copy Management System and CGMS: Copy Generation Management System are famous.

Copy free (Copy Free) which shows that the copy is permitted without restriction in such copy control information as for the data in which the information was added. Information including the copy prohibition (Copy Prohibited) etc. which do not accept the one-generation copy permission (One Generation Copy Allowed) which permits the copy of only one generation and a copy can be expressed.

[0102] Example 3 shown in drawing 10 is an example which makes ATS 24 bits uses 2 bits of CCI(s) and uses 6 bits of information of further others. As other information when the analog output of this data is carried out for example it is possible to use various information including information etc. which shows ON and OFF (On/Off) of the macro vision (Macrovision) which is a copy control mechanism of an analog video data.

[0103] [Tree (Thurs.) structure as key distribution composition] Next the composition which distributes the key which needs it when the recording and reproducing device shown in drawing 1 reproduces data from record or a recording medium to a recording medium for example a medium key to each apparatus is explained. Drawing 11 is a figure showing the distribution composition of the key of the recording and reproducing device in the recording system which used this method. The numbers 0-15 shown in the bottom of drawing 11 are each recording and reproducing devices. That is each leaf (leaf: leaf) of the tree (tree) structure shown in drawing 11 is equivalent to each recording and reproducing device.

[0104] Each devices 0-15 store in person the key (node key) assigned to the node of a to [ from its own leaf in the initial tree defined beforehand / a route ] and the leaf key of each leaf at the time of manufacture (at the time of shipment). K0000-K1111 which are shown in the bottom of drawing 11 are the leaf key assigned to each devices 0-15 respectively and let key: KR-K111 indicated in the 2nd paragraph (node) from the bottom be a node key from KR of the highest rung.

[0105] In the tree composition shown in drawing 11 the device 0 owns the leaf key K0000 node key: K000 and K00K0 and KR. The device 5 K0101 K010 K01K0 and KR are owned. The device 15 owns K1111 K111 K11K1 and KR. Although 16 devices of 0-15 are indicated to the tree of drawing 11 and the tree structure is also shown as symmetrical composition which was able to take balance of 4 stage constitution it is possible to have number-of-stages composition which much more devices are

constituted in a tree and is different in each part of a tree.

[0106] The record reproducer various type which uses various recording media for example DVDCDMDa memory stick (trademark) etc. is contained in each record reproducer contained in the tree structure of drawing 11. It is assumed that various application services live together. The key distribution composition shown in drawing 11 after such a different device and different application constitute [coexistence] is applied.

[0107] In the system by which these various devices and application live together the portion 012 and 3 enclosed with the dotted line of drawing 11 i.e. devices is set up as one group using the same recording medium. For example the device contained in the group enclosed with this dotted line is received. It collects and common contents are enciphered and processing in which send the master key which is sent from a provider or is used in common or encipher to a provider or a settlement-of-accounts organization too and the payment data of a content rate is outputted to it from each device is performed. Organizations which perform data transmission and reception with each device such as a content provider or a settlement processing organization perform the portion enclosed with the dotted line of drawing 11 i.e. the processing which bundle up the devices 012 and 3 as one group and sends data. Two or more such groups exist in the tree of drawing 11.

[0108] A node key and a leaf key are good also as composition managed for every group with the provider who may generalize and manage by one certain lock management center and performs various data transmission and reception to each group a settlement-of-accounts organization etc. As for these node keys and a leaf key in disclosure of a key etc. an update process is performed and a lock management center a provider a settlement-of-accounts organization etc. perform this update process.

[0109] In this tree structure the three devices 012 and 3 contained in one group hold the key K00 common as a node key K0 and KR so that clearly from drawing 11. By using this node key share composition it becomes possible to provide only the devices 012 and 3 with a common master key for example. For example if node key K00 the very thing held in common is set up as a master key setting out of a master key only with the common devices 012 and 3 is possible without performing new key sending. If the value Enc (K00 Kmaster) which enciphered the new master key Kmaster by the node key K00 is stored in a recording medium via a network and distributed to the devices 012 and 3 Only the devices 012 and 3 become possible [solving the code Enc (K00 Kmaster) using the share node key K00 held in each device and obtaining master key: Kmaster]. It is shown that Enc (Ka Kb) is the data which enciphered Kb by Ka.

[0110] When it is revealed in t at a certain time that key: K0011 which the device 3 owns K001 K00 K0 and KR were analyzed by the aggressor (hacker) and it was exposed of KRAfter it in order to protect the data transmitted and received by a system (group of the devices 012 and 3) it is necessary to separate the device 3 from a system. for that purpose -- a node key -- : -- K -- 001 -- K -- 00 -- K --

-- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of generation (Generation):t of the key Kaaa.

[0111]Distribution processing of an updating key is explained. The renewal of a key the table constituted by the block data called the validation key blocks (EKB:Enabling Key Block) shown in drawing 12 (A)for example For examplea networkOr it performs by storing in a recording medium and supplying the devices 01and 2.

[0112]It is constituted as block data which has a data configuration which can update only the required device of renewal of a node key in the validation key blocks (EKB) shown in drawing 12 (A). In the devices 01and 2 in the tree structure shown in drawing 11the example of drawing 12 is the block data formed for the purpose of distributing the generation's t updating node key. drawing 11 -- from -- being clear -- as -- a device -- zero -- a device -- one -- updating -- a node key -- \*\*\*\*\* -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- required -- a device -- two -- updating -- a node key -- \*\*\*\*\* -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- being required .

[0113]As shown in EKB of drawing 12 (A)two or more cryptographic keys are contained in EKB. The cryptographic key of the bottom is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- self -- having -- a leaf key -- this -- a cryptographic key -- decoding -- K -- (-- t --) -- 001 -- it can obtain . using K(t)001 obtained by decodingdecoding of the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) is attained from under drawing 12 (A)and updating node key K(t)00 can be obtained. belowone by onethe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. on the other hand -- a device -- zero -- one -- a node key -- K -- 000 -- updating -- an object -- containing -- not having -- updating -- a node key -- \*\*\*\*\* -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is . The devices 0 and 1 decode the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 12 (A)and acquire K(t)00hereafterthe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. Thus the devices 01and 2 can obtain updated key K(t) R. The index of drawing 12 (A) shows the actual address of the node key and leaf key which are used as a decryption key.

[0114]The node key of the upper stage of the tree structure shown in drawing 11 : when renewal of K(t) 0 and K (t) R is unnecessary and the update process of only



the node key K00 is required by using the validation key blocks (EKB:Enabling Key Block) of drawing 12 (B) updating node key K(t)00 can be distributed to the devices 01 and 2.

[0115] EKB shown in drawing 12 (B) is available when distributing a medium key peculiar to the new master key shared for example in a specific group or a recording medium. As an example the recording medium with the devices 01 and 3 in the group who shows by a dotted line is used for drawing 11 and suppose that new common master key K(t) master is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (t) -- 00 -- using -- being new -- being common -- updating -- a master key -- : -- K -- (t) -- master -- having enciphered -- data -- Enc (K (t) K(t) master) -- drawing 12 -- (B) -- being shown -- EKB -- distributing . By this distribution the distribution as data of the device 4 etc. which is not decoded in other groups' apparatus is attained. The same may be said of a medium key.

[0116] That is if the devices 01 and 2 decode the above-mentioned cryptogram using K(t)00 which processed and obtained EKB it will become possible to obtain master key: K(t) master in t time and medium key: K(t) media.

[0117] [Acquisition of the medium key which uses EKB] as an example of processing which obtains medium key K(t) media in t time proposed to drawing 13 by Japanese Patent Application No. 2000-105328 which is the patent application of these people's point K (t) Processing of the device 2 which received EKB shown in the data Enc (K(t) 00 and K (t) media) which enciphered new common medium key K(t) media using 00 and drawing 12 (B) via the recording medium is shown.

[0118] As shown in drawing 11 suppose that four devices of the devices 01 and 3 surrounded by the dotted line are contained in a certain recording and reproducing system. When are RIBOKU the device 3 and using the medium key assigned for every recording medium drawing 13 The processing at the time of asking for a medium key required in order that a recording and reproducing device (device 2) may encipher or decode the contents on a recording medium using the debye skiing which EKB (Enabling Key Block) stored in the recording medium and a recording and reproducing device memorize is expressed.

[0119] The leaf key K\_0010 assigned only to itself and the node key (respectively K\_001K\_00K\_0K\_R) of each nodes 00100 and 0R from it to a wooden route are safely stored in the memory of the device 2. The device 2 calculates node key K(t)\_001 of the node 001 by index (index) decoding the cryptogram of 0010 among EKB(s) stored in the recording medium of drawing 13 by the leaf key K\_0010 which he has Next it needs to calculate medium key K(t)\_media using it by decoding the cryptogram of 001 and index (index) calculating node key K(t)\_00 of the node 00 using it finally and decoding a cryptogram. These calculation times increase in proportion to the depth to the node which enciphers a medium key from a leaf becoming deep. That is in the big system by which many recording and reproducing devices exist many calculations are needed. Thus the data encryption processing and the decoding processing mode using the medium key calculated and acquired

are explained hereafter.

[0120][Contents recording processing using a medium key] According to the processing block figure of drawing 14 an example of encryption processing of the data which the cipher-processing means 150 performs and the recording processing to a recording medium is explained.

[0121]The recording and reproducing device 100 shown in drawing 14 acquires a medium key by calculation processing based on EKB which self mentioned above.

[0122]Next it is inspected whether as for the recording and reproducing device 100 disk ID (Disc ID) as identification information is already recorded on the recording medium 200 which is an optical disc. If recorded disk ID (Disc ID) is read and if not recorded for example it was set at random or beforehand in the cipher-processing means 150 disk ID (Disc ID) will be generated by methods such as a random number generation and it will record on a disk. The thing with one stored in read in area etc. since it is good is also possible for disk ID (Disc ID) on the disk.

[0123]A medium key and disk ID are used for the record reproducer 100 next and it generates a disk inherent key (Disc Unique Key). As a concrete generation method of a disk inherent key (Disc Unique Key) The method of Example 1 using the result obtained by inputting a medium key and disk ID (Disc ID) into the hash function using a block cipher function as shown in drawing 15 To hash function SHA-1 defined by FIPS 180-1. The data generated by the bit connection to a medium key and disk ID (Disc ID) is inputted and the method of Example 2 which uses only required data length as a disk inherent key (Disc Unique Key) from the output of 160 bits can be applied.

[0124]Next for example title key (Title Key) which is an inherent key for every record was defined at random or beforehand in the cipher-processing means 150 (refer to drawing 1) it generates by methods such as a random number generation and records on the disk 200.

[0125]Next the combination of title key (Title Key) to a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key) are generated.

[0126]The concrete method of this title inherent key (Title Unique Key) generation The method of Example 1 using the result obtained by enciphering a title key by using a disk inherent key as a key using a block cipher function as shown in drawing 16 To hash function SHA-1 defined by FIPS 180-1. The data generated by the bit connection to a medium key and disk ID (Disc ID) is inputted and the method of Example 2 which uses only required data length as a title inherent key (Title Unique Key) from the output of 160 bits can be applied.

[0127]In the above-mentioned explanation a disk inherent key (Disc Unique Key) is generated from a medium key and disk ID (Disc ID) Although he is trying to generate a title inherent key (Title Unique Key) from this and the title key (Title Key) respectively a title inherent key (Title Unique Key) being directly generated from a medium key disk ID (Disc ID) and the title key (Title Key) using a disk inherent key (Disc Unique Key) as unnecessary and A key equivalent to a title inherent key (Title Unique Key) may be generated from a medium key (Master Key)

and disk ID (Disc ID) without using the title key (Title Key).

[0128] Subsequent processing is explained using drawing 14. The block seed (Block Seed) whose 1–4th byte of the head of the block data is inputted as encrypted data is separated and is outputted from the title inherent key (Title Unique Key) generated previously. The block key (Block Key) which is a key which enciphers the data of the block is generated.

[0129] The example of the generation method of block key (Block Key) is shown in drawing 17. By drawing 17 each shows two examples which generate the 64-bit block key (Block Key) from 32 bits block seed (Block Seed) and a 64-bit title inherent key (Title Unique Key).

[0130] 64 bits of key length and the code function whose input and output are 64 bits respectively are being used for Example 1 shown in the upper row. A title inherent key (Title Unique Key) is used as the key of this code function and the result which is inputted the value which connected the constant (constant) of 32 bits with block seed (Block Seed) and was enciphered is made into the block key (Block Key).

[0131] Example 2 is an example which used hash function SHA-1 of FIPS 180-1. The value which connected the block seed (Block Seed) with the title inherent key (Title Unique Key) is inputted into SHA-1. What was contracted to 64 bits such as 64 bits of low ranks accepting the output of 160 bits and using it for example is made into the block key (Block Key).

[0132] Although the example which generates a disk inherent key (Disc Unique Key), a title inherent key (Title Unique Key) and the block key (Block Key) above respectively was explained, for example without performing generation of a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key) the block key (Block Key) may be generated using a medium key, disk ID (Disc ID), title key (Title Key) and the block seed (Block Seed) for every block.

[0133] Generation of a block key will encipher block data using the generated block key (Block Key). As shown in the lower berth of drawing 14 it dissociates (selector 1608) and the 1st – m byte (for example m = 8 bytes) of the head of block data including the block seed (Block Seed) do not consider it as the candidate for encryption but enciphers from the m+1st byte to final data. In m byte which is not enciphered the 1–4th byte as BURROKU seed is also contained. The block data after the m+1st byte separated by the selector is enciphered according to the encryption algorithm beforehand set as the cipher-processing means 150. As an encryption algorithm DES (Data Encryption Standard) specified for example by FIPS 46-2 can be used.

[0134] Contents are block units and encryption is given by the above processing with the block key generated based on the medium key by which generation management was carried out, block seed etc. and they are stored in a recording medium by it.

[0135] Next to the recorded enciphered content data a recording and reproducing device calculates a digital signature using the secret key (signature generating key) of a public-key-encryption system assigned to self and records this on a

recording medium with an own public key certification and contents data. As a generation method of a digital signature EC-DNA (Elliptic Curve Digital Signature Algorithm) under standard establishment can be used by IEEE P1363 for example. The flow chart explaining the outline of the recording processing of contents is shown in drawing 18.

[0136] First a recording and reproducing device performs encryption processing of recording object contents in Step S101. Contents encryption is performed as encryption processing of the block data using a block key as explained using drawing 14.

[0137] In Step S102a recording and reproducing device calculates the digital signature to enciphered content using the secret key (signature generating key) of a public-key-encryption system assigned to self. As a generation method of a digital signature EC-DNA (Elliptic Curve Digital Signature Algorithm) under standard establishment is applicable by IEEE P1363 for example.

[0138] Next in Step S103a recording and reproducing device matches with record contents the digital signature and public key certification which were generated and records them on a recording medium and recording processing (S102) to the recording medium of encryption data is performed in Step S104.

[0139] The detailed process flow in the case of performing a digital signature to enciphered content and performing record is shown in drawing 19.

[0140] In Step S201a recording and reproducing device acquires a medium key by the above-mentioned EKB processing (refer to drawing 13).

[0141] In S202 it is inspected whether disk ID (Disc ID) as identification information is already recorded on the recording medium. If are recorded and this disk ID is read and it is not recorded by S203 by S204 disk ID is generated by the method defined at random or beforehand and it records on a disk. Next in S205a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1 the method (refer to drawing 15) of using the hash function based on a block cipher etc.

[0142] Next it progresses to S206 and the title key (Title Key) as a peculiar key for the one record of every is generated and the generated title key is recorded on a disk (recording medium). Next by S207a title inherent key is generated from the above-mentioned disk inherent key and a title key (refer to drawing 16).

[0143] A recording and reproducing device receives S208 the encrypted data of the contents data which should be recorded in the form of a TS packet. By S209 TS processing means 300 adds ATS which is the time information which received each TS packet. Or the value which combined the copy control information CCI and ATS and the information of further others is added. Next it is judged whether the TS packet which added ATS was received one by one by S2101 block is formed for example the identification data in which whether it having amounted to  $X = 32$  and the end of a packet are shown was received. When one of conditions is satisfied it progresses to Step S211 and the packet to X individual or the end of a packet is put in order and 1-block block data is formed.

[0144]Nextthe cipher-processing means 150 is S212 and generates the block key which is a key which enciphers the data of the block from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S207 (refer to drawing 17).

[0145]In S213the block data formed by S211 using the block key is enciphered. As explained also in advanceit is the m+1st byte to final data of block data that it is the target of encryption. DES (Data Encryption Standard) as which an encryption algorithm is specifiedfor example by FIPS 46-2 is applied.

[0146]By S214it judges whether a recording block is the 1st blockand when it is the 1st blockin S215a digital signature is generated by using block data as digital signature object dataand it records on a recording medium with a public key certification. The generation processing of a digital signature applies EC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment for exampleby IEEE P1363.

[0147]By S216the enciphered block data is recorded on a recording medium. By S217it is judged whether all the data was recorded. If all the data is recordedrecording processing is ended and all the data is not recordedit will return to S208 and processing of the remaining data will be performed.

[0148]Contents will be enciphered by the above processingit will be recorded on a recording mediumand the digital signature to the block data of enciphered content and a public key certification will be further recorded on a recording medium.

[0149]The contents stored in a recording mediuma title keya DEJITASHIRU signaturea public key certificationand other contents associated data are recorded with composition identifiable in each correspondence. For exampleit can match by recording on a recording medium by using management data as a table. The example of a table format in the case of recording the address information of the associated data about record contents as a table is shown in drawing 20.

[0150]As shown in drawing 20each contents with contents associated data. It is managed as a filethe address of contents datathe address of a title keythe address of a digital signaturethe address of a public key certificationand the other tables recorded about file information are generatedand it is stored in a recording medium.

[0151]Nextwhen recording enciphered content on a recording mediumthe processing which does not perform a signature to enciphered contentbut performs a digital signature to the title key generated corresponding to contentsand performs contents recording is explained using the flow of drawing 21.

[0152]In Step S301a recording and reproducing device acquires a medium key by the above-mentioned EKB processing (refer to drawing 13).

[0153]In S302it is inspected whether disk ID (Disc ID) as identification information is already recorded on the recording medium. If are recordedand this disk ID is read and it is not recorded by S303by S304disk ID is generated by the method defined at random or beforehandand it records on a disk. Nextin S305a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash

function SHA-1 defined by FIPS 180-1 the method (refer to drawing 15) of using the hash function based on a block cipher etc.

[0154] Next it progresses to S306 and the title key (Title Key) as a peculiar key for the one record of every is generated and the digital signature to the generated title key is performed. The generation processing of a digital signature applies EC-DSA (Elliptic Curve Digital Signature Algorithm) under standard establishment for example by IEEE P1363. The title key digital signature and public key certification which were generated are stored in a recording medium (disk).

[0155] Next by S307 a title inherent key is generated from the above-mentioned disk inherent key and a title key (refer to drawing 16).

[0156] A recording and reproducing device receives S308 the encrypted data of the contents data which should be recorded in the form of a TS packet. By S309 TS processing means 300 adds ATS which is the time information which received each TS packet. Or the value which combined the copy control information CCI and ATS and the information of further others is added. Next it is judged whether the TS packet which added ATS was received one by one by S310 1 block is formed for example the identification data in which whether it having amounted to X= 32 and the end of a packet are shown was received. When one of conditions is satisfied it progresses to Step S311 and the packet to X individual or the end of a packet is put in order and 1-block block data is formed.

[0157] Next the cipher-processing means 150 is S312 and generates the block key which is a key which enciphers the data of the block from 32 bits (block seed containing ATS) of the head of block data and the title inherent key generated by S307 (refer to drawing 17).

[0158] In S313 the block data formed by S311 using the block key is enciphered. As explained also in advance it is the m+1st byte to final data of block data that it is the target of encryption. DES (Data Encryption Standard) as which an encryption algorithm is specified for example by FIPS 46-2 is applied.

[0159] By S314 the enciphered block data is recorded on a recording medium. By S315 it is judged whether all the data was recorded. If all the data is recorded recording processing is ended and all the data is not recorded it will return to S308 and processing of the remaining data will be performed.

[0160] Contents will be enciphered by the above processing it will be recorded on a recording medium and the digital signature to the title key corresponding to enciphered content and a public key certification will be further recorded on a recording medium.

[0161] Although the digital signature was given to the title key in the above-mentioned example a digital signature may be given to a title key and disk ID. By doing in this way it can clarify that the data was recorded on the disk and that by which the data was copied to other disks can make easily judgment that it is an unjust copy.

[0162] [Contents playback processing using a medium key] Next decoding of enciphered content data and regeneration which were stored in the recording medium are explained below using drawing 22.

[0163]In regeneration playback equipment reads the public key certification and digital signature of a recorder which are first recorded with the contents data to reproduce and checks such justification.

[0164]That is if the justification of a public key certification is inspected using the public key (signature verification keys) of a reliable center which playback equipment holds and it succeeds in this the digital signature which the recorder created and recorded using the public key (signature verification keys) of a recorder contained in the public key certification will be inspected. As an inspection method of a digital signature above-mentioned EC-DSA can be used for example.

[0165]Next playback equipment reads the identification information (ID) of a recorder from the public key certification currently recorded and checks that RIBOKU (exclusion) of this recorder is not carried out from a system from this and RIBOKESHON information.

[0166](RIBOKU inspection using a RIBOKESHON list) As RIBOKESHON information the RIBOKESHON list shown for example in drawing 23 can be used. A center gives a digital signature to the data which wrote together ID of the apparatus which carries out RIBOKU (exclusion) as a RIBOKESHON list is shown in a figure and the version number of a list. For example the memory of the apparatus (recording and reproducing device) by which 1 manufacture is carried out is made to memorize this RIBOKESHON list. It is made to circulate via a network or a recording medium together with 2 contents data. It enables it to acquire the RIBOKESHON information that playback equipment is newer by circulating the inside of a system by which method at the time of regeneration.

[0167]When using a RIBOKESHON list in order to inspect that a list is not what was forged and altered verification processing of a signature of the center stored in the RIBOKESHON list is performed. The verification processing of a signature can be inspected like signature verification of a public key certification using the public key (signature verification keys) of the center which apparatus (recording and reproducing device) has beforehand.

[0168](RIBOKU inspection using EKB) It is good also as composition which does not take the composition distributed to each apparatus as a list as RIBOKESHON information shown in drawing 23 again but distinguishes RIBOKU using EKB. For example in the system by which apparatus has been arranged at the tree form shown in drawing 11 it is assumed that EKB shown in the example 1 of (A) of drawing 12 was stored in the recording medium. If each apparatus sees the index of EKB one by one at this time he can understand that what expressed with tree form the node key updated by EKB becomes like the thick line of drawing 24.

[0169]And he gets blocked only the apparatus located under the leaf (leaf) of the tree shown by the thick line and that the updated node key can be obtained can understand that they are only the devices 01 and 2. And RIBOKU [ the other apparatus / system ] can be judged. It becomes possible to suspend redistribution of the record contents by RIBOKU apparatus by performing processing which forbids reproduction of the contents data which apparatus with these ID recorded

at the time of execution of regeneration. It is premised on the position of the leaf in drawing 11 and ID of a device corresponding in this example. That is the existence of RIBOKU is distinguished by performing trace processing of the index of validation key blocks (EKB) based on said ID.

[0170] The RIBOKU inspection by trace processing is explained in detail. First the example of a format of validation key blocks (EKB) is shown in drawing 25. The version 1001 is an identifier which shows the version of validation key blocks (EKB). A version has a function which shows the correspondence relation of the function and contents which identify the newest EKB. The depth 1002 shows the hierarchy number of the hierarchy tree to the device of the distribution destination of validation key blocks (EKB). The data pointer 1003 is a pointer in which the position of the data division in validation key blocks (EKB) is shown. It is a pointer which the tag pointer 1004 shows the position of a tag part to and the signature pointer 1005 shows the position of a signature.

[0171] The data division 1006 stores the data which enciphered the node key updated (for example, for example each cryptographic key about the updated node key as shown in drawing 13 is stored).

[0172] The tag part 1007 is a tag in which the physical relationship of the node key and leaf key which were stored in the data division and which were enciphered is shown. The grant rule of this tag is explained using drawing 26. Drawing 26 shows the example which sends the validation key blocks (EKB) previously explained by drawing 12 (A) as data. The data at this time comes to be shown in the table (b) of drawing 26. Let the address of the top node contained in the cryptographic key at this time be a top node address. In this case since updating key  $K(t)$  R of the route key is contained a top node address serves as KR. At this time the data  $\text{Enc}(K(t)0)$  and  $K(t)R$  of the highest rung is in the position shown in the hierarchy tree shown in (a) of drawing 26 for example. Here the following data is  $\text{Enc}(K(t)00K(t)0)$ . It is in the position at the lower left of front data on a tree.

A tag is set up and 1 is set up when there is data and there is nothing 0 and. A tag is set up as [a left (L) tag and a right (R) tag]. Since there is data in the left of the data  $\text{Enc}(K(t)0)$  and  $K(t)R$  of the highest rung and there is no data in L tag = 0 and the right it is set to R tag = 1. Hereafter a tag is set as all the data and the data row shown in drawing 26 (c) and a tag sequence are constituted.

[0173] A tag is a key arrangement identification tag set up in order to show where [ of a tree structure ] the data  $\text{Enc}(K_{xxx}K_{yyy})$  is located. the key data  $\text{Enc}(K_{xxx}K_{yyy})$  stored in a data division -- since ... is only enumeration data of the key enciphered simply it enables distinction of the position on the tree of the cryptographic key stored as data with the tag mentioned above. The node index to which encryption data was made to correspond like composition of that previous drawing 12 explained is used without using the tag mentioned above for example it is 0:  $\text{Enc}(K(t)0)$  and  $K(t)$  root).

00:  $\text{Enc}(K(t)00K(t)0)$

000:  $\text{Enc}(K(t)000K(t)00)$



Although it is also possible to consider it as a data configuration like ...in the distribution etc. which it will become redundant data and data volume will increase if it has composition using such an index and pass a network it is not desirable. On the other hand distinction of a key position is attained with small data volume by using the tag mentioned above as index data in which a key position is shown.

[0174]It returns to drawing 25 and an EKB format is explained further. A signature (Signature) is an electronic signature which the EKB issue office which published validation key blocks (EKB) for example a certificate authority a lock management center contents ROBAIDA a settlement-of-accounts organization etc. perform. It checks that the devices which received EKB are the validation key blocks (EKB) which the just validation key-blocks (EKB) publisher published by signature verification.

[0175]The tag stored in EKB so that I might be understood from the explanation about drawing 26 shows 0 or 1 existence of the key data of the left of a self-node and a right node. That is when there is data the case where there are not 0 and data is set up as 1. The tracking processing of EKB based on leaf ID i.e. how to follow is performed using the tag based on such conditioning.

[0176]Pursuit (how to follow) of EKB based on leaf ID is explained using drawing 27. Let the device which has the leaf key K1001 as shown in drawing 27 (a) be a RIBOKU device [1001]. At this time EKB has the composition of a cryptographic key like drawing 27 (b) and a tag. EKB of drawing 27 (b) turns into EKB which updated KRK1K10 and K100 in order RIBOKU [one device [1001] of drawing 27 (a)].

[0177]By processing this EKB all leaves other than a RIBOKU device [1001] can acquire updated route key K(t) R. That is since the leaf which stands in a row in the low rank of the node key K0 holds in a device the node key K0 which is not updated the acquisition of updating route key K(t) R of it is attained by decoding  $\text{Enc}(K0K(t)R)$  by K0. The leaf not more than K11 acquires updating node key K(t)1 using K11 which is not updated by decoding  $\text{Enc}(K11K(t)1)$  by K11. An updating route key is acquirable by decoding  $\text{Enc}(K(t)1 \text{ and } K(t)R)$  by K(t)1. Only by one decoding step increasing also about the low rank leaf of K101 an updating route key is acquirable similarly.

[0178]It is a self leaf key and the device [1000] with the leaf key [RIBOKU / leaf key] K1000 decodes  $\text{Enc}(K1000K(t)100)$  after acquiring K(t)100 it decodes the node key of a higher rank one by one and can acquire an updating route key.

[0179]RIBOKU -- having had -- a device -- [ -- 1001 -- ] -- self -- a leaf -- one -- a step -- a top -- updating -- a node key -- K -- ( -- t -- ) -- 100 -- EKB -- processing -- being unacquirable -- since -- after all -- updating -- a route -- a key -- K -- ( -- t -- ) -- R -- being unacquirable .

[0180]The data division shown in drawing 27 (b) and EKB which has a tag are distributed to the just device [RIBOKU / device] from an EKB issue office and it is stored in the device.

[0181]The device which tries to perform RIBOKU verification acquires ID from a public key certification after verification of the public key certification of the

RIBOKU device [ID=1001] of drawing 27 (a). This ID is [1001] and shows the leaf position of EKB distribution tree composition.

[0182]The device which took out ID [1001] verifies whether the device corresponding to the leaf of ID=1001 is set up as an effective leaf device in EKB. It performs as processing which judges whether route key K(t) R by which this verification [1001]i.e.a leafwas updated is acquirable.

[0183]For exampleif it is a leaf belonging to the low rank of the renewal node keys of un-(K0 of ex. drawing 27 (a)K11etc.)When it is a leaf which can judge if RIBOKU is clear and it is a just deviceand belongs to the low rank of an updating node keyA judgment RIBOKU [ whether the encryption data which can acquire the updating node key is stored in EKB / the entity ] is attained.

[0184]The example which performs EKB tracking processing as an example of decision processing based on the tag stored in EKB is explained. EKB tracking processing is processing which judges whether a key distribution tree can be followed from the route key of a higher rank. For exampleaccording to a lower bita tree is followed for [1001] which is ID of the leaf [1001] of drawing 27 as 4 bits of [1][0][0]and [1] one by one from the most significant bit. If a bit is 1 and it is right-hand side and 0it will progress to the left.

[0185]From the route of drawing 27 (a)the most significant bit of ID [1001] is 1and goes to right-hand side. The tag of the beginning in EKB is 0: {00}and having data on both branches is judgedit goes to right-hand sideand it is followed and stuck to K1. Nextit progresses to the node of the low rank of K1. The 2nd bit of ID [1001] is 0 and goes to left-hand side. It is 2: {00} of drawing 27 (a) and (b)and it judges that the tag in which the data existence of the low rank of K1 is shown has data on both branchesand it goes to left-hand sideand is followed and stuck to K10. The 3rd bit of ID [1001] is 0 and goes to left-hand side. It is 3: {00} of drawing 27 (a) and (b)and it judges that the tag in which the data existence of the low rank of K10 is shown has data on both branchesand it goes to left-hand sideand is followed and stuck to K100. The least significant bit of ID [1001] is 1and goes to right-hand side. The tag in which the data existence of the low rank of K100 is shown is 5: {01} of drawing 27 (a) and (b)and does not have data in right-hand side. thereforearrive at a node [1001] -- it is judged that there is nothing and it is judged with the device of ID [1001] being the device which cannot acquire the updating route key by EKBi.e.a RIBOKU device.

[0186]For exampleif the device ID which has the leaf key K1000 of drawing 27 (a) is [1000] and the EKB tracking processing based on the tag in the same EKB as \*\*\*\*i.e.the processing which follows a treeis performedSince it can arrive at a node [1000]it is judged with it being a just device [ RIBOKU / device ] which can acquire the updating route key by EKB.

[0187]arrive also at the leaf of low rankssuch as the node key which is not updatedfor examplefor exampleK0and K11at the leaf itself -- although there is nothingit is possible to arrive at the end node which is not updated in this case. Since processing of EKB is possible for the leaf of the low rank of the node which is not updated and it can acquire an updating route key using the node key which

is not updated it is a just device. It becomes possible [ judging with the tag corresponding to the node ] whether it is a node key which is not updated. The tag corresponding to the node key K0 which is not updated K11 and K101 is set to 1: {11}4: {11} and 6 {11} and although a low order node or a leaf exists further these Not having enciphered key data in EKB is shown and it is judged with the device of the leaf of the low rank of these being an effective just device [ RIBOKU / device ].

[0188] Although the example shown in drawing 27 is a RIBOKU mode only about one device it is also possible RIBOKU [ all the leaf devices which are under a certain node as shown in drawing 28 ] collectively. The data (cryptographic key) of EKB in this case and a tag become like drawing 28 (b).

[0189] For example supposing it acquires ID [1000] from the public key certification of the leaf device corresponding to K1000 [ RIBOKU / 1000 / the device ] processing which follows a tree based on the tag of EKB based on this ID [1000] will be performed.

[0190] From the route of drawing 28 (a) the most significant bit of ID [1000] is 1 and goes to right-hand side. It is tag 0 of the beginning in EKB: {00} and having data on both branches is judged it goes to right-hand side and it follows and sticks to K1. Next it progresses to the node of the low rank of K1. The 2nd bit of ID [1000] is 0 and goes to left-hand side. The tag in which the data existence of the low rank of K1 is shown is 2: {10} of drawing 13 (a) and (b) and does not have data in left-hand side. therefore arrive at a node [1000] -- there is nothing. The tags corresponding to the end node K1 at this time are {10} and are not {11} without low-ranking data.

[0191] The tag {10} shows that the enciphered key data for acquiring K1 (t) which can be decoded and which was updated only in the right-hand side low-ranking node or leaf of K1 is stored in EKB.

[0192] Thus the final point which arrives based on leaf ID is a node and when the correspondence tag of the last node has values other than {11} having low-ranking enciphered key data in EKB further is shown. In this case since the leaf device with that ID cannot acquire the route key updated by processing of EKB it is judged with it being the device [ RIBOKU / device ].

[0193] Thus it becomes possible to judge RIBOKU [ the communications partner ] based on leaf ID stored in the public key certification acquired from the communications partner in authenticating processing.

[0194] The process flow using EKB about RIBOKU device decision processing is shown in drawing 29. Each step of a flow is explained. In Step S351 ID is acquired from a public key certification to be examined. In Step S352 tracking processing aiming at the leaf or lead which ID shows based on the tag of EKB using acquired ID is performed.

[0195] Tracking processing is performed in the procedure explained using above-mentioned drawing 27 and drawing 28. as a result of tracking processing arrive at the leaf or node which ID shows or arrive -- even if it is a case where there is nothing in the leaf or node which ID shows it is judged whether acquisition of whether EKB processing is possible and an updating route key is possible (S353).

[0196] If judged with it being ID in the position in which EKB processing is

possible it will progress to Step S354 and will judge with the device corresponding to ID being a just device [ RIBOKU / device ]. If judged with it being ID which is in the position in which EKB processing is impossible on the other hand it will progress to Step S355 and will judge with the device corresponding to ID being an inaccurate device [ RIBOKU / device ].

[0197] In above-mentioned tracking processing although the tag part of EKB uses the data division does not use. Size of EKB for them can be made small by using not the usual EKB shown in drawing 25 but EKB without a data division using this in order to express RIBOKESHON information. Of course it is also possible to use EKB for protecting the usual contents shown in drawing 25 since RIBOKESHON information is expressed.

[0198] As mentioned above that verification which does not require RIBOKU [ the apparatus which recorded contents to the recording medium by the RIBOKU inspection according to a RIBOKESHON list or trace processing of an EKB tree ] is performed. On condition that RIBOKU [ the apparatus which recorded contents ] was verified playback equipment continues regeneration of contents data. Like the encryption and recording processing which were explained using drawing 14 from a medium key and disk ID in regeneration generate a disk inherent key and A disk inherent key A title inherent key is generated from a title key further from a title key and the block seed read in a recording medium a block key is generated and decoding processing of the encryption data of the block unit read in the recording medium 200 is performed using a block key as a decryption key.

[0199] The outline of regeneration is explained using the flow chart of drawing 30. First in Step S401 playback equipment performs the public key certification of a storing salmon \*\*\*\* contents recording device and verification of a digital signature to the recording medium which recorded reproduction object contents. After performing the center signature of a public key certification using the public key of a center and checking the justification of a public key certification first verification takes out the public key of the contents recording device stored in the public key certification and performs verification of a contents recording person's digital signature. Any verification follows that to the following step by O.K. if one of verification is NG subsequent stepwise execution is forbidden and regeneration is stopped.

[0200] Next the RIBOKESHON inspection of a contents recording device is performed in Step S402. This RIBOKESHON inspection is conducted by inspecting whether apparatus ID stored in the RIBOKESHON list shown in drawing 23 beforehand stored in playback equipment for example and apparatus ID in a public key certification have a match. Or tree search processing by the above-mentioned EKB tree composition may be performed. If judged with RIBOKU [ the contents recording device ] in the RIBOKESHON inspection of Step S402 when RIBOKU [ the following step / progress and ] subsequent stepwise execution is forbidden and regeneration is stopped.

[0201] When judged with RIBOKU [ the contents recording device ] in the

RIBOKESHON inspection of Step S402In Step S403read-out from the recording medium of enciphered content is performeddecoding processing of enciphered content is performed in Step S404and reproduction of contents is performed.

[0202]Thussince it had composition which performs only reproduction of the contents recorded by the apparatus [ RIBOKU / apparatus / by judging the RIBOKU situation of a contents recording device ] on the occasion of the contents playback processing stored in the recording mediumIt is prevented that circulation use of the contents recorded unjustly is carried out disorderly. A RIBOKU judging is judged by ID stored in the public key certificationand the reliability is maintained.

[0203]Nextthe detailed processing in the case of performing reproduction of the record contents by which the digital signature was performed to enciphered content using drawing 31 is explained.

[0204]In Step S501playback equipment reads a medium key and disk ID from a recording mediumand performs read-out of a title keya digital signatureand a public key certification in Step S502. When a signature and a public key certification do not exist (S503:No)it is judged with their not being the contents by just recording processingexecution of subsequent processings is suspendedand regeneration is ended.

[0205]When a signature and a public key certification exist (S503:Yes)verification of a public key certification is performed in Step S504. Verification of a public key certification is performed using the public key of the center (certificate authority) which performs issue management of the public key certification which playback equipment holds. Verification of a public key certification is O.K.and if justification is checkedit will progress to the following step. When justification verification is NGexecution of subsequent processings is suspended and regeneration is ended.

[0206]Nextin Step S505the identifier (ID) of a recorder which performed contents recording is taken out from a public key certificationand a RIBOKU inspection is conducted. A RIBOKU inspection is performed by either Libor Christo of above-mentioned drawing 23or tree search processing. If judged with there being no RIBOKU of the recorder of contentsit will progress to the following stepand if judged with those with RIBOKUexecution of subsequent processings will be suspended and regeneration will be ended.

[0207]Nextin S506a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1the method (refer to drawing 15) of using the hash function based on a block cipheretc.

[0208]Nextit progresses to S507 and a title inherent key is generated from the title key which read and read the title key (Title Key)and a disk inherent key (refer to drawing 16).

[0209]In S508playback equipment reads the block data of the contents data which should be reproduced. It reads by S509 and judges whether a block is the 1st blockand in being the 1st blockit performs verification of a contents recording person's (recorder) digital signature generated to the 1st block in Step S510.

Verification of a digital signature is performed using the public key of the contents recording device picked out from the public key certification in which justification was verified. Verification of a digital signature is O.K. and if justification is checked it will progress to the following step. When justification verification is N.G. execution of subsequent processings is suspended and regeneration is ended.

[0210] In Step S511 the block key which is a key which decodes the data of the block is generated from 32 bits (block seed containing ATS) of the head of block data and the title inherent key generated by S507 (refer to drawing 17).

[0211] In S512 block data is decoded using a block key. DES (Data Encryption Standard) as which a decoding algorithm is specified for example by FIPS 46-2 is applied.

[0212] By S513 it is judged whether all the data was read. If all the data is read regeneration is ended and all the data is not read it will return to S508 and processing of the remaining data will be performed.

[0213] Thus verification of a public key certification the judgment of RIBOKU of a contents recording device Sequential execution of the verification of the digital signature to the block data of enciphered content will be carried out the justification of contents will be judged based on all the conditions having been satisfied and decoding from the recording medium of enciphered content and regeneration will be performed.

[0214] Next the detailed processing in the case of performing reproduction of the record contents by which the digital signature was performed to the title key using drawing 32 is explained.

[0215] In Step S601 playback equipment reads a medium key and disk ID from a recording medium and performs read-out of a title key a digital signature and a public key certification in Step S602. When a signature and a public key certification do not exist (S603:No) it is judged with their not being the contents by just recording processing execution of subsequent processings is suspended and regeneration is ended.

[0216] When a signature and a public key certification exist (S603:Yes) verification of a public key certification is performed in Step S604. Verification of a public key certification is performed using the public key of the center (certificate authority) which performs issue management of the public key certification which playback equipment holds. Verification of a public key certification is O.K. and if justification is checked it will progress to the following step. When justification verification is N.G. execution of subsequent processings is suspended and regeneration is ended.

[0217] Next in Step S605 the identifier (ID) of a recorder which performed contents recording is taken out from a public key certification and a RIBOKU inspection is conducted. A RIBOKU inspection is performed by either Libor Christo of above-mentioned drawing 23 or tree search processing. If judged with there being no RIBOKU of the recorder of contents it will progress to the following step and if judged with those with RIBOKU execution of subsequent processings will be suspended and regeneration will be ended.

[0218] Next verification of a contents recording person's (recorder) digital signature

performed to the title key in Step S606 is performed. Verification of a digital signature is performed using the public key of the contents recording device picked out from the public key certification in which justification was verified. Verification of a digital signature is O.K. and if justification is checked it will progress to the following step. When justification verification is NG execution of subsequent processings is suspended and regeneration is ended.

[0219] Next in S607 a disk inherent key is generated using a medium key and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1 the method (refer to drawing 15) of using the hash function based on a block cipher etc.

[0220] Next it progresses to S608 and a title inherent key is generated from the title key which read and read the title key (Title Key) and a disk inherent key (refer to drawing 16).

[0221] In S609 playback equipment reads the block data of the contents data which should be reproduced. In Step S610 the block key which is a key which decodes the data of the block is generated from 32 bits (block seed containing ATS) of the head of block data and the title inherent key generated by S608 (refer to drawing 17).

[0222] In S611 block data is decoded using a block key. DES (Data Encryption Standard) as which a decoding algorithm is specified for example by FIPS 46-2 is applied.

[0223] By S612 it is judged whether all the data was read. If all the data is read regeneration is ended and all the data is not read it will return to S609 and processing of the remaining data will be performed.

[0224] Thus verification of a public key certification the judgment of RIBOKU of a contents recording device Sequential execution of the verification of the digital signature to the title key of enciphered content will be carried out the justification of contents will be judged based on all the conditions having been satisfied and decoding from the recording medium of enciphered content and regeneration will be performed.

[0225] As mentioned above in the encryption processing at the time of the record over the recording medium of contents data and the decoding processing at the time of the reproduction from a recording medium Based on the medium key which computed the medium key based on EKB and was computed after that other identifiers etc. the key for encryption processing of contents or the key for decoding processings is generated.

[0226] Although the example mentioned above explained the composition which generates the key used for contents data encryption processing and decoding processing using a medium key It is good also as composition which generates the key which acquires not a medium key but a master key common to two or more recording and reproducing devices or debye skiing peculiar to a record reproducer from EKB and uses it for contents data encryption processing and decoding processing based on these. It is also possible to apply as the medium key acquired from EKB a master key or a key which uses the debye skiing itself for encryption

processing of contents data and decoding processing.

[0227]As mentioned abovein this inventionwhen a recording and reproducing device recorded data on an information recording mediuman own digital signature and public key certification were recorded with data. Since he is trying to also certainly record with data proof which recorder recordedby this when recording informationSince it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulatedexclusion from a system can be performed.

[0228]When a recording and reproducing device reads dataafter checking the justification of the above-mentioned digital signature and the public key certification and checking RIBOKU [ the recorder / system ] furtherit had composition which reads data. While the inaccurate recorder is delivering the powerless thing an attack which does not record a digital signature to inaccurate record data by thisexclusion from the system of an inaccurate device is more powerfully performed by making it not reproduce the data recorded with an inaccurate device with a just device.

[0229][Copy control in recording processing Nowin order to protect profitssuch as an owner of a copyright of contentsin the licensed deviceit is necessary to control the copy of contents.]

[0230]That isto record contents on a recording mediumthe contents investigate whether it is what may be copied (a copy is possible)and it is necessary to make it record only the contents which may be copied. When reproducing and outputting the contents recorded on the recording mediumthe illegal copy of the contents to output needs to be made not to be carried out later.

[0231]Thenprocessing of the recording and reproducing device of drawing 1 in the case of performing record reproduction of contents is explained with reference to the flow chart of drawing 33 and drawing 34performing copy control of such contents.

[0232]Firstwhen recording the contents of the digital signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 33 (A) is performed. Processing of drawing 33 (A) is explained. The record reproducer 100 of drawing 1 is explained as an example. If the contents (digital contents) of a digital signal are supplied to input-and-output I/F120 via an IEEE1394 serial bus etc.in Step S701input-and-output I/F120 will receive the digital contentsand they will follow it to Step S702for example.

[0233]In Step S702it is judged whether the digital contents which received can copy input-and-output I/F120. That isthe contents are judged [ that it can copy and ] when the contents which input-and-output I/F120 received are not enciphered for example (for examplewhen the contents of a plaintext are supplied to input-and-output I/F120without using above-mentioned DTCP).

[0234]It shall suppose that the recording and reproducing device 100 is a device based on DTCPand processing shall be performed according to DTCP. 2-bit EMI (Encryption Mode Indicator) as copy control information for controlling a copy is prescribed by DTCP. When EMI is 00B (B expresses that the value before that is a



binary number)Contents express that it is copy-free (Copy-freely)and when EMI is 01Bcontents express that it is what (No-more-copies) cannot carry out the copy beyond it. It expresses that contents are what (Copy-one-generation) may be copied only once when EMI is 10Band when EMI is 11Bcontents express that it is what (Copy-never) the copy is forbidden.

[0235]EMI is contained in the signal supplied to input-and-output I/F120 of the recording and reproducing device 100and contents are judged [ that it can copy and ] when the EMI is Copy-freely and Copy-one-generation. Contents are judged [ that it cannot copy and ] when EMI is No-more-copies and Copy-never.

[0236]In Step S702when judged [ that contents cannot be copied and ]Steps S703-S705 are skippedand recording processing is ended. Thereforecontents are not recorded on the recording medium 10 in this case.

[0237]In Step S702when judged [ that contents can be copied and ]it progresses to Step S703 and processing in Step S12 of drawing 3 (A)S13and S14 and same processing are hereafter performed in Steps S703-S705. That isATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means 150 are performedthe enciphered content obtained as a result is recorded on the recording medium 195and recording processing is ended.

[0238]EMI is contained in the digital signal supplied to input-and-output I/F120. When digital contents are recordedthe informationincluding for exampleembedded CCI in DTCPetc.which expresses a copy control state like EMI or EMI with the digital contents is also recorded.

[0239]Under the present circumstancesgenerallythe information showing Copy-One-Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed.

[0240]In the recording and reproducing device of this inventioncopy control informationsuch as this EMIembedded CCIetc.is recorded in the form added to a TS packet. That islike Example 2 of drawing 10or Example 332 bits which added 24 bits thru/or 30 bitsand copy control information for ATS are added to each TS packetas shown in drawing 5.

[0241]When recording the contents of the analog signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 33 (B) is performed. Processing of drawing 33 (B) is explained. When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S711the analog content which received the analog contentand progressed and received to Step S712 judges whether it can copy or not.

[0242]Here the decision processing of Step S712 to the signal received by input-and-output I/F140for example. It is carried out based on whether a macro vision (Macrovision) signal and a CGMS-A (Copy Generation Management System-Analog) signal are included. That iswhen a macro vision signal is recorded on the video cassette tape of a VHS methodit is a signal which serves as a noise.

Analog content is judged [ that it cannot copy and ] when this is contained in the signal received by input-and-output I/F140.

[0243]For example a CGMS-A signal is a signal which applied the CGMS signal used for the copy control of a digital signal to the copy control of the analog signal. It is expressed any of what (Copy-freely) has a free copy of contents, the thing (Copy-one-generation) which may be copied only once or the things (Copy-never) to which the copy is forbidden they are.

[0244]Therefore analog content is judged [ that it can copy and ] when a CGMS-A signal is included in the signal received by input-and-output I/F140 and the CGMS-A signal expresses Copy-freely and Copy-one-generation. Analog content is judged [ that it cannot copy and ] when the CGMS-A signal expresses Copy-never.

[0245]Analog content is judged [ that it can copy and ] when a macro vision signal and CGMS-A signal is not included in the signal received by input-and-output I/F4 for example either.

[0246]In Step S712 when judged [ that analog content cannot be copied and ] Steps S713 thru/or S717 are skipped and recording processing is ended.

Therefore contents are not recorded on the recording medium 10 in this case.

[0247]In [ when judged / that analog content can be copied and / progress to Step S713 in Step S712 and ] the following and Steps S713 thru/or S717 Processing in Steps S22 thru/or S26 of drawing 3 (B) and same processing are performed and thereby digital conversion, MPEG coding, TS processing and encryption processing are made and contents are recorded on a recording medium and end recording processing.

[0248]When the CGMS-A signal is included in the analog signal received by input-and-output I/F140 and analog content is recorded on a recording medium, the CGMS-A signal is also recorded on a recording medium. That is, this signal is recorded on the portion of the information on CCI shown by drawing 10 or others. Under the present circumstances, generally, the information showing Copy-One-Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed. However, it is not this limitation when a rule such as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies" is decided in the system.

[0249][Copy control in regeneration] Next, when reproducing the contents recorded on the recording medium and outputting outside as digital contents, regeneration according to the flow chart of drawing 34 (A) is performed. Processing of drawing 34 (A) is explained. In Step S801, S802 and S803, processing in Step S31 of drawing 4 (A), S32 and S33 and same processing are performed first and by this, in the cipher-processing means, 150 decoding processing is made for the enciphered content read from the recording medium and TS processing is made. The digital contents by which each processing was performed are supplied to input-and-output I/F120 via the bus 110.

[0250]Input-and-output I/F120 judges whether it is what the digital contents

supplied there can copy later in Step S804. That is the contents are judged [ that it can copy later and ] when the information (copy control information) which expresses a copy control state to the digital contents supplied to input-and-output I/F120 like EMI or EMI for example is not included.

[0251] When EMI is contained in the digital contents supplied to input-and-output I/F120 for example. Therefore when EMI is recorded according to the standard of DTCP at the time of record of contents. Digital contents are judged [ that it can copy later and ] when the EMI (recorded EMI (Recorded EMI)) is Copy-freely. Contents are judged [ that it cannot copy later and ] when EMI is No-more-copies.

[0252] Generally recorded EMI is neither Copy-one-generation nor Copy-never. It is because the digital contents which EMI of Copy-one-generation is changed into No-more-copies at the time of record and have EMI of Copy-never are not recorded on a recording medium. However it is not this limitation when a rule such as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies" is decided in the system.

[0253] In Step S804 when contents are judged [ that it can copy later and ] it progresses to Step S805 and input-and-output I/F120 outputs the digital contents outside and ends regeneration.

[0254] When contents are judged [ that it cannot copy later and ] in Step S804 progress to Step S806 and input-and-output I/F120. For example according to the standard of DTCP etc. it outputs outside in the form where digital contents are not copied to the digital contents later and regeneration is ended.

[0255] Namely when EMI recorded as mentioned above for example is No-more-copies (or although the copy control information of "Copy-one-generation is recorded in a system without changing into No-more-copies) The rule of treating as No-more-copies" is decided and when EMI recorded under the conditions is Copy-one-generation as for contents the copy beyond it is not allowed.

[0256] For this reason input-and-output I/F120 attests mutually between a partner's devices according to the standard of DTCP when a partner is a just device enciphers digital contents (when it is a device based on the standard of DTCP here) and outputs them outside.

[0257] Next when reproducing the contents recorded on the recording medium and outputting outside as analog content regeneration according to the flow chart of drawing 34 (B) is performed. Processing of drawing 34 (B) is explained. In Steps S811 thru/or S815 processing in Steps S41 thru/or S45 of drawing 4 (B) and same processing are performed. That is read-out of enciphered content decoding processing TS processing MPEG decoding and D/A conversion are performed. The analog content obtained by this is received by input-and-output I/F140.

[0258] Input-and-output I/F140 judges whether it is what the contents supplied there can copy later in Step S816. That is the contents are judged [ that it can copy later and ] when copy control information such as EMI is not recorded on the contents currently recorded together for example.

[0259] Contents are judged [ that it can copy later and ] when EMI or copy control

information is recorded for example according to the standard of DTCP at the time of record of contents and the information is Copy-freely.

[0260]When EMI or copy control information is No-more-copies in a system record the copy control information of "Copy-one-generation without changing into No-more-copies but. The rule of treating as No-more-copies" is decided and contents are judged [ that it cannot copy later and ] when EMI or copy control information recorded under the conditions is Copy-one-generation.

[0261]When a CGMS-A signal is included in the analog content supplied to input-and-output I/F140 for example Therefore analog content is judged [ that it can copy later and ] when a CGMS-A signal is recorded with the contents at the time of record of contents and the CGMS-A signal is Copy-freely. Analog content is judged [ that it cannot copy later and ] when a CGMS-A signal is Copy-never.

[0262]In Step S816 when contents are judged [ that it can copy later and ] it progresses to Step S817 and input-and-output I/F140 outputs outside the analog signal supplied there as it is and ends regeneration.

[0263]In Step S816 when contents are judged [ that it cannot copy later and ] it progresses to Step S818 and input-and-output I/F140 is outputted outside in the form where analog content is not copied to the analog content later and ends regeneration.

[0264]Namely when copy control informations such as EMI recorded as mentioned above for example is No-more-copies (or) Although the copy control information of "Copy-one-generation is recorded in a system without changing into No-more-copies The rule of treating as No-more-copies" is decided and when copy control informations such as EMI recorded under the conditions is Copy-one-generation as for contents the copy beyond it is not allowed.

[0265]For this reason input-and-output I/F140 adds the GCMS-A signal with which a macro vision signal and Copy-never are expressed for analog content at it for example and outputs it outside. For example also when the recorded CGMS-A signal is Copy-never as for contents the copy beyond it is not allowed. For this reason input-and-output I/F140 changes a CGMS-A signal into Copy-never and outputs it outside with analog content.

[0266]As mentioned above it becomes possible by performing record reproduction of contents to prevent the copy (illegal copy) besides the range which contents were allowed from being performed performing copy control of contents.

[0267][Composition of a data processing means] Software can also perform as well as in addition performing a series of processings mentioned above by hardware. That is it is also possible to have composition performed by making a general-purpose computer and the microcomputer of one chip execute a program for example although the cipher-processing means 150 can also be constituted as encryption/decoding LSI. TS processing means 300 can perform processing with software similarly. When software performs a series of processings the program which constitutes the software is installed in a general-purpose computer the microcomputer of one chip etc. Drawing 35 shows the example of composition of the 1 embodiment of the computer by which the program which performs a series

of processings mentioned above is installed.

[0268]A program is recordable on hard disk [ as a recording medium ] 2005 and ROM 2003 built in the computer beforehand. A program Or a floppy (registered trademark) disk CD-ROM (Compact Disc Read Only Memory) It is temporarily or permanently storable in the removable recording media 2010 such as MO (Magneto optical) disk DVD (Digital Versatile Disc) a magnetic disk and semiconductor memory (record). Such a removable recording medium 2010 can be provided as what is called a software package.

[0269]Install a program in a computer from the removable recording medium 2010 which was mentioned above and also via the artificial satellite for the digital satellite broadcasting from a download site Via networks [ \*\*\*\* / transmitting to a computer on radio ] such as LAN (Local Area Network) and the Internet It transmits to a computer with a cable and in a computer it can receive in the communications department 2008 and the program transmitted by making it such can be installed on the hard disk 2005 to build in.

[0270]The computer contains CPU (Central Processing Unit) 2002. The input/output interface 2011 is connected to CPU 2002 via the bus 2001. CPU 2002 via the input/output interface 2010 by a user. If instructions are inputted by operating the input part 2007 which comprises a keyboard a mouse etc. according to it the program stored in ROM (Read Only Memory) 2003 will be executed.

[0271]Or a program by which CPU 2002 is stored in the hard disk 2005 A program which was transmitted from the satellite or the network was received in the communications department 2008 and was installed on the hard disk 2005 Or the program which was read from the removable recording medium 2010 with which the drive 2009 was equipped and was installed on the hard disk 2005 is loaded to RAM (Random Access Memory) 2004 and is executed.

[0272]Thereby CPU 2002 performs processing performed by the composition of the block diagram according to the flow chart mentioned above processed or mentioned above. CPU 2002 the processing result and via the input/output interface 2011 if needed It is made to record on an output or the transmission from the communications department 2008 and also the hard disk 2005 from the outputting part 2006 which comprises LCD (Liquid Crystal Display) a loudspeaker etc.

[0273]The processing step which describes the program for making various kinds of processings perform to a computer in this Description here It is not necessary to necessarily process to a time series in accordance with the order indicated as a flow chart and a parallel target or the processing (for example parallel processing or processing by an object) performed individually is also included.

[0274]A program may be processed by the computer of 1 and distributed processing may be carried out by two or more computers. A program may be transmitted to a distant computer and may be executed.

[0275]Although this embodiment explained as a center the example which

constitutes the block which performs encryption/decoding of contents from encryption/decoding LSI of one chip. The block which performs encryption/decoding of contents can also be realized as one software module which CPU170 shown in drawing 1 performs for example. It is possible similarly to also realize processing of TS processing means 300 as one software module which CPU170 performs.

[0276] As mentioned above, it has explained in detail about this invention referring to specific working example. However, it is obvious that a person skilled in the art can accomplish correction and substitution of this working example in the range which does not deviate from the gist of this invention. That is, with the gestalt of illustration, this invention has been indicated and it should not be interpreted restrictively. In order to judge the gist of this invention, the column of the Claims indicated at the beginning should be taken into consideration.

[0277]

[Effect of the Invention] As mentioned above, as explained when the Information Storage Division device records data on an information recording medium according to the composition of this invention, an own digital signature and public key certification are recorded with data. By this, when recording information, proof which recorder recorded was also always recorded with data. It checks that an information reproducing device checks the justification of a signature and a public key certification and specifies a contents recording person before the decoding processing of contents, and there is no alteration of a public key certification and a digital signature in it. By this composition, efficient exclusion of use (reproduction) of the record contents by an inaccurate recorder is attained. Since it can specify which recorder recorded it even if the recording medium containing the data recorded unjustly circulated, exclusion from a system can be performed.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the example of composition of the Information Storage Division playback equipment of this invention.

[Drawing 2] It is a figure showing the example of the public key certification applied in the Information Storage Division playback equipment of this invention.

[Drawing 3] It is a figure showing the Data Recording Sub-Division process flow of the Information Storage Division playback equipment of this invention.

[Drawing 4] It is a figure showing the data reproduction process flow of the Information Storage Division playback equipment of this invention.

[Drawing 5] It is a figure explaining the data format processed in the Information Storage Division playback equipment of this invention.

[Drawing 6] It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 7]It is a figure explaining the composition of the transport stream processed in the Information Storage Division playback equipment of this invention.

[Drawing 8]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 9]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 10]It is a figure showing the example of composition of the block data as additional information of block data processed in the Information Storage Division playback equipment of this invention.

[Drawing 11]It is a tree lineblock diagram explaining the EKB message distribution processing to the Information Storage Division playback equipment of this invention.

[Drawing 12]It is a figure showing the example of EKB used for the key distribution to the Information Storage Division playback equipment of this invention.

[Drawing 13]It is a figure showing the example of distribution which uses EKB of the medium key in the Information Storage Division playback equipment of this inventionand the example of decoding processing.

[Drawing 14]It is a block diagram explaining the encryption processing at the time of the Data Recording Sub-Division processing which uses the medium key in the Information Storage Division playback equipment of this invention.

[Drawing 15]It is a figure which illustrates the example of generation of an applicable disk inherent key in the Information Storage Division playback equipment of this invention.

[Drawing 16]In the Information Storage Division playback equipment of this inventionit is a figure showing the example of generation processing of an applicable title inherent key.

[Drawing 17]It is a figure which illustrates the generation method of an applicable block key in the Information Storage Division playback equipment of this invention.

[Drawing 18]It is a block diagram explaining the encryption processing at the time of the Data Recording Sub-Division processing in the Information Storage Division playback equipment of this invention.

[Drawing 19]It is a flow chart explaining the processing which generates the signature to enciphered content in the Information Storage Division playback equipment of this inventionand performs Data Recording Sub-Division.

[Drawing 20]It is a figure showing the example of composition of the enciphered content recorded in the Information Storage Division playback equipment of this inventionand the table which manages correspondence with a public key certificationa signatureetc.

[Drawing 21]It is a flow chart explaining the processing which generates the signature to a title key in the Information Storage Division playback equipment of this inventionand performs Data Recording Sub-Division.

[Drawing 22]It is a block diagram explaining the decoding processing at the time of

the data reproduction processing in the Information Storage Division playback equipment of this invention.

[Drawing 23]It is a figure showing the example of composition of the RIBOKESHON table used in the Information Storage Division playback equipment of this invention.

[Drawing 24]It is a figure explaining the processing in the case of carrying out application \*\* of the EKB distribution tree in the Information Storage Division playback equipment of this invention at the inspection of a RIBOKU device.

[Drawing 25]It is a figure showing the example of a format of applicable validation key blocks (EKB) in the Information Storage Division playback equipment of this invention.

[Drawing 26]It is a figure explaining the composition of the tag of validation key blocks (EKB).

[Drawing 27]It is a figure (Example 1) explaining the EKB tracking processing for a RIBOKU entity judging.

[Drawing 28]It is a figure (Example 2) explaining the EKB tracking processing for a RIBOKU entity judging.

[Drawing 29]It is a flow chart explaining the EKB tracking processing for a RIBOKU entity judging.

[Drawing 30]It is a flow chart explaining the processing which verifies a signature in the Information Storage Division playback equipment of this inventionand performs data reproduction.

[Drawing 31]It is a flow chart explaining the processing which verifies the signature to enciphered content in the Information Storage Division playback equipment of this inventionand performs data reproduction.

[Drawing 32]It is a flow chart explaining the processing which verifies the signature to a title key in the Information Storage Division playback equipment of this inventionand performs data reproduction.

[Drawing 33]It is a flow chart explaining the copy control processing at the time of the Data Recording Sub-Division processing in the Information Storage Division playback equipment of this invention.

[Drawing 34]It is a flow chart explaining the copy control processing at the time of the data reproduction processing in the Information Storage Division playback equipment of this invention.

[Drawing 35]In the Information Storage Division playback equipment of this inventionit is a block diagram showing the processing means composition in the case of performing data processing with software.

[Description of Notations]

100 Recording and reproducing device

110 Bus

120 Input-and-output I/F

130 MPEG codec

140 Input-and-output I/F

141 A/Da D/A converter



150 Cipher-processing means  
160 ROM  
170 CPU  
180 Memory  
190 Drive  
200 Recording medium  
210 Recording-medium I/F  
300 TS processing means  
600607 Terminal  
602 Bit stream purser  
603 PLL  
604 Time stamp generation circuit  
605 Block seed additional circuit  
606 Smoothing buffer  
800806 Terminal  
801 Block seed separation circuits  
802 Output controlling circuit  
803 Comparator  
804 Timing generating circuit  
805 27 MHz clocks  
901904913 Terminal  
902 MPEG video encoder  
903 Video stream buffer  
905 MPEG audio encoder  
906 Audio stream buffer  
908 Multiplexing scheduler  
909 Transport packet coding equipment  
910 Arrival-time-stamps calculating means  
911 Block seed additional circuit  
912 Smoothing buffer  
976 Switch  
1001 Version  
1002 Depth  
1003 Data pointer  
1004 Tag pointer  
1005 Signature pointer  
1006 Data division  
1007 Tag part  
1008 Signature  
2001 Bus  
2002 CPU  
2003 ROM  
2004 RAM  
2005 Hard disk

2006 Outputting part  
2007 Input part  
2008 Communications department  
2009 Drive  
2010 Removable recording medium  
2011 Input/output interface

---

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-236622  
(P2002-236622A)

(43) 公開日 平成14年8月23日 (2002. 8. 23)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7 3 2 0 F 5 J 1 0 4
G 0 9 C 1/30	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B

審査請求 未請求 請求項の数24 O L (全 42 頁)

(21) 出願番号 特願2001-34969 (P2001-34969)

(22) 出願日 平成13年2月13日 (2001. 2. 13)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

Fターム(参考) 5B017 AA06 BA07 BA09 CA09

5J104 AA01 AA09 AA16 EA02 EA04

EA26 LA03 LA06 NA02 NA05

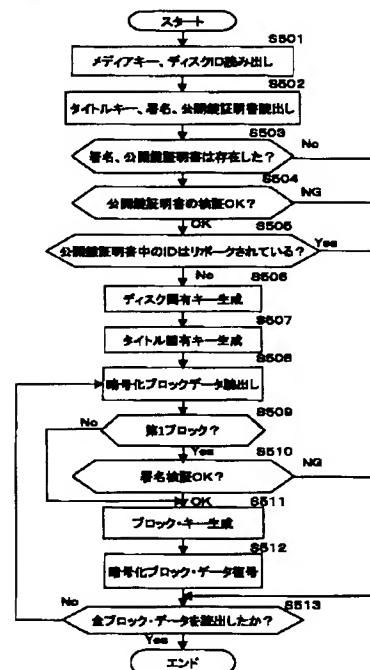
PA14

(54) 【発明の名称】 情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体

(57) 【要約】

【課題】 コンテンツ再生において、正当な記録コンテンツ記録であるか否かを判定して再生する構成を持つ情報記録再生装置および方法を提供する。

【解決手段】 データを情報記録媒体に記録する際にデジタル署名および公開鍵証明書を記録し、コンテンツを記録した記録装置を特定可能とした。不正に記録されたデータを含む記録媒体が流通しても、記録装置を特定しシステムからの排除が行える。情報再生装置は、データを読み出す際に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認した後にデータを再生する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。



## 【特許請求の範囲】

【請求項1】記録媒体から情報を再生する情報再生装置において、

前記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置。

【請求項2】前記暗号処理手段は、前記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項1に記載の情報再生装置。

【請求項3】前記暗号処理手段は、前記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項1に記載の情報再生装置。

【請求項4】前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キープロック（EKB）の復号を実行して前記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する構成を有することを特徴とする請求項1に記載の情報再生装置。

【請求項5】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項4に記載の情報再生装置。

【請求項6】記録媒体に対して情報を記録する情報記録装置において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置。

【請求項7】前記情報記録装置は、

格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記録媒体に格納する処理を実行する構成を有することを特徴とする請求項6に記載の情報記録装置。

【請求項8】前記暗号処理手段は、前記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項6に記載の情報記録装置。

【請求項9】前記暗号処理手段は、前記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする請求項6に記載の情報記録装置。

【請求項10】前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キープロック（EKB）の復号を実行して前記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする請求項6に記載の情報記録装置。

【請求項11】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする請求項10に記載の情報記録装置。

【請求項12】記録媒体から情報を再生する情報再生方法において、前記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、を有することを特徴とする情報再生方法。

【請求項13】前記情報再生方法における前記署名検証ステップは、前記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として

暗号化コンテンツの復号処理を実行することを特徴とする請求項 12 に記載の情報再生方法。

【請求項 14】前記情報再生方法における前記署名検証ステップは、

前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする請求項 12 に記載の情報再生方法。

【請求項 15】前記情報再生方法は、さらに、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キーブロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする請求項 12 に記載の情報再生方法。

【請求項 16】記録媒体に対して情報を記録する情報記録方法において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書に対応付けて記録媒体に格納するステップと、を有することを特徴とする情報記録方法。

【請求項 17】前記情報記録方法は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスに対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする請求項 16 に記載の情報記録方法。

【請求項 18】前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項 16 に記載の情報記録方法。

【請求項 19】前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする請求項 16 に記載の情報記録方法。

【請求項 20】前記情報記録方法は、さらに、前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キーブロック（EKB）の復号を実行

して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする請求項 16 に記載の情報記録方法。

【請求項 21】暗号化コンテンツを格納した情報記録媒体であり、

該暗号化コンテンツを記録した記録主体の識別データと、

前記記録主体の公開鍵証明書と、

前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体。

【請求項 22】前記情報記録媒体は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスに対応付けた管理テーブルを格納したことを特徴とする請求項 21 に記載の情報記録媒体。

【請求項 23】記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、

正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、

該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、

を有することを特徴とするプログラム記憶媒体。

【請求項 24】記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、

前記格納コンテンツの記録主体のデジタル署名を生成するステップと、

暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書に対応付けて記録媒体に格納するステップと、

を有することを特徴とするプログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関し、特に、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、また情報記

録装置がリボークされていないことを確認した後にデータを読み出す構成とした情報再生装置、情報記録装置、情報再生方法、情報記録方法、および情報記録媒体、並びにプログラム記憶媒体に関する。

#### 【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0003】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】しかしながら、SCMSは上述のようにS

CMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0006】コンテンツ・スクランブルシステムでは、DVD-ROM（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行えないことになり、不正コピーが防止されるようになっている。

【0008】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0009】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘

密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0012】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【0014】しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0015】上記問題を解決する構成として、本出願人は、各情報記録再生装置を $n$ 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平2000-105328）している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えば $n$ 分木の各

葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な態様で暗号化処理した情報を含む有効化キーブロック（EKB）を各情報記録再生装置に配信し、有効化キーブロック（EKB）を受信した各情報記録再生装置のEKB復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【0016】

【発明が解決しようとする課題】上記の構成においては、秘密が露呈した装置をシステムから排除することは可能であるが、このためにはどの装置の秘密が露呈したかを特定する必要がある。たとえば、ある装置から盗んだ秘密を搭載したクローンデバイスが作られ、ブラックマーケットで販売されていたことが特定できれば、秘密を盗まれた装置が特定され、システムから排除されることになる。

【0017】ところで、システムに対する攻撃を考えると、上記のようにクローンデバイスが作られて出まわるのではなく、ある情報記録装置を改造して、たとえば本来は暗号化して記録すべきデータを平文で記録するなどの、不正な記録を行わせて、その結果作られた、不正に記録されたデータを含む記録媒体を販売するなどの行為が考えられる。この場合、その記録媒体にデータを不正に記録した装置が特定できれば、それをシステムから排除し、新しいコンテンツデータをその装置では復号させないように配信することが、上記の方法で可能である。

【0018】本発明は、上述の問題を解決するものであり、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録し、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とすることにより、コンテンツ記録が正当に行われたものであることを条件として再生を可能とするシステムを提供することを目的とする。

【0019】

【課題を解決するための手段】本発明の第1の側面は、記録媒体から情報を再生する情報再生装置において、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行し、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする情報再生装置にある。

【0020】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処

理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【0021】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行し、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【0022】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報再生装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キープロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する構成を有することを特徴とする。

【0023】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【0024】さらに、本発明の第2の側面は、記録媒体に対して情報を記録する情報記録装置において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理手段を有し、該暗号処理手段は、前記格納コンテンツの記録主体のデジタル署名を生成し、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納する処理を実行する構成を有することを特徴とする情報記録装置にある。

【0025】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

【0026】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納する構成であることを特徴とする。

【0027】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに

対応付けて格納する構成であることを特徴とする。

【0028】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記情報記録装置に内蔵したキーに基づいてキーツリーのパス上の下位キーによる上位キーの暗号化処理データからなる有効化キープロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する構成を有することを特徴とする。

【0029】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または記録媒体に固有のメディアキーであることを特徴とする。

【0030】さらに、本発明の第3の側面は、記録媒体から情報を再生する情報再生方法において、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、正当性の確認された公開鍵証明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、を有することを特徴とする情報再生方法にある。

【0031】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツのコンテンツを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【0032】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法における前記署名検証ステップは、前記記録媒体に格納された暗号化コンテンツに対応して設定されるタイトルキーを署名対象として生成されたコンテンツ記録主体のデジタル署名の検証処理を実行するステップを含み、該検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行することを特徴とする。

【0033】さらに、本発明の情報再生方法の一実施態様において、前記情報再生方法は、さらに、複数の異なる情報再生装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーに基づいて、有効化キープロック（EKB）の復号を実行して前記記録媒体に格納された暗号データの復号処理に必要な復号キー生成用データを取得する処理を実行することを特徴とする。



【0034】さらに、本発明の第4の側面は、記録媒体に対して情報を記録する情報記録方法において、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、を有することを特徴とする情報記録方法にある。

【0035】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを生成し、前記記録媒体に格納する処理を実行することを特徴とする。

【0036】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツのコンテンツを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【0037】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記記録媒体に格納する暗号化コンテンツに対応して設定されるタイトルキーを署名対象としてコンテンツ記録主体のデジタル署名の生成処理を実行し、生成した署名を格納コンテンツに対応付けて格納することを特徴とする。

【0038】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、前記情報記録装置に内蔵した複数の異なる情報記録装置をリーフとした階層キーツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに基づいて有効化キープロック（EKB）の復号を実行して前記記録媒体に格納するデータの暗号化処理に必要な暗号化キー生成用データを取得する処理を実行することを特徴とする。

【0039】さらに、本発明の第5の側面は、暗号化コンテンツを格納した情報記録媒体であり、該暗号化コンテンツを記録した記録主体の識別データと、前記記録主体の公開鍵証明書と、前記記録主体のデジタル署名とを格納したことを特徴とする情報記録媒体にある。

【0040】さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、格納コンテンツ、デジタル署名、公開鍵証明書のアドレスを対応付けた管理テーブルを格納したことを特徴とする。

【0041】さらに、本発明の第6の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、前記記録媒体に格納された暗号化コンテンツ記録主体の公開鍵証明書の検証処理を実行する公開鍵証明書検証ステップと、正当性の確認された公開鍵証

明書から前記コンテンツ記録主体の公開鍵を取得して、該取得した公開鍵に基づいて、コンテンツ記録主体のデジタル署名の検証処理を実行する署名検証ステップと、該署名検証の結果、署名の正当性が確認されたことを条件として暗号化コンテンツの復号処理を実行するステップと、を有することを特徴とするプログラム記憶媒体にある。

【0042】さらに、本発明の第7の側面は、記録媒体に対して情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを格納したプログラム記憶媒体であって、前記コンピュータ・プログラムは、記録媒体に格納するコンテンツの暗号化処理を実行する暗号処理ステップと、前記格納コンテンツの記録主体のデジタル署名を生成するステップと、暗号化コンテンツ、デジタル署名および、暗号化コンテンツ記録主体の公開鍵証明書を対応付けて記録媒体に格納するステップと、を有することを特徴とするプログラム記憶媒体にある。

【0043】

【作用】本発明においては、情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【0044】さらに、情報再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしている。すなわち、記録されたデータに対して有効なデジタル署名がなければ、正当な再生装置はそのデータを再生しないからである。

【0045】

【発明の実施の形態】〔システム構成〕図1は、本発明を適用した記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、入出力I/F（Interface）120、MPEG（Moving Picture Experts Group）コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F（Interface）140、暗号処理手段150、ROM（Read Only Memory）160、CPU（Central Processing Unit）170、メモリ180、記録媒体200の記録媒体インタフェース（I/F）190、さらにトランスポート・ストリーム処理手段（TS処理手段）300を有し、これらはバス110によって相互に接続されている。

【0046】入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成す

るデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【0047】暗号処理手段150は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0048】ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。さらに、記録再生装置固有の、公開鍵暗号系の秘密鍵と、公開鍵証明書、さらに、信頼できるセンタの公開鍵を記憶しておく。

【0049】ここで、公開鍵証明書は、図2に示すように、その証明書利用者、例えば記録再生装置のIDと、利用者の公開鍵を格納し、その他のデータをメッセージとして信頼できるセンタ(認証局)がデジタル署名を施したデータである。センタのデジタル署名の検証処理を、予め取得済みのセンタの公開鍵を用いて実行して公開鍵証明書の正当性が確認でき、格納された公開鍵を取り出して利用することができる。

【0050】CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。記録媒体インタフェース190は、デジタルデータを記録再生可能な記録媒体200を駆動することにより、記録媒体200からデジタルデータを読み出し(再生し)、バス110上に出力するとともに、バス1

10を介して供給されるデジタルデータを、記録媒体200に供給して記録させる。また、プログラムをROM160に、デバイスキー等をメモリ180に記憶する構成としてもよい。

【0051】記録媒体200は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース190に対して着脱可能な構成であるとする。但し、記録媒体200は、記録再生装置100に内蔵する構成としてもよい。

【0052】トランスポート・ストリーム処理手段(TS処理手段)300は、後段において図を用いて詳細に説明するが、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリームから特定のプログラム(コンテンツ)に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体200に格納するためのデータ処理および、記録媒体200からの再生処理時の出現タイミング制御処理を行なう。

【0053】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのATS(Arrival Time Stamp:着信時刻スタンプ)が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるTSSTD(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段(TS処理手段)300は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段(TS処理手段)300は、DVD等の記録媒体200へのデータ記録時に、各トランスポートパケットの入力タイミングを表すATS(Arrival Time Stamp:着信時刻スタンプ)を付加して記録する。

【0054】なお、本発明の処理システムにおいて処理されるデータはトランスポートストリームに従ったフォーマット・データに限られるものではない。従ってトランスポートストリーム以外のデータに関する処理を実行する場合は、図1に示すTS処理手段は必ずしも必要とはならない。

【0055】〔データ記録処理およびデータ再生処理〕次に、図1の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理につ

いて、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体200に記録する場合においては、図3(A)のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS11において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、TS処理手段300または、暗号処理手段150に出力する。

【0056】受信データがトランスポートストリーム処理を必要とする場合は、TS処理手段300においてトランスポート・ストリーム処理が実行される。TS処理手段300は、ステップS12において、トランスポートストリームを構成する各トランスポートパケットにATSを付加したブロックデータを生成して、バス110を介して、暗号処理手段150に出力する。この処理については、さらに後段で詳細に説明する。

【0057】暗号処理手段150は、ステップS13において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、記録媒体I/F190に出力する。暗号化コンテンツは、記録媒体I/F190を介して記録媒体200に記録(S14)され、記録処理を終了する。

【0058】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、SCDTCF(Five Company Digital Transmission Content Protection)(以下、適宜、DTCFという)が定められているが、このDTCFでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ(暗号化コンテンツ)を復号するようになっている。

【0059】このDTCFに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS11で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCFに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0060】DTCFによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝

送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0061】なお、DTCFによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCFについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメショナルバージョン(Informational Version)の取得が可能である。

【0062】次に、外部からのアナログ信号のコンテンツを、記録媒体200に記録する場合の処理について、図3(B)のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS21において、そのアナログコンテンツを受信し、ステップS22に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

【0063】このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS23において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

【0064】以下、ステップS24、S25、S26において、図3(A)のステップS12、S13、S14における処理と同様の処理が行われる。すなわち、必要であればTS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体200に記録して、記録処理を終了する。

【0065】次に、記録媒体200に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図4のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図4(A)のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップS31において、記録媒体I/F190によって、記録媒体200に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0066】暗号処理手段150では、ステップS32

において、記録媒体1/F190から供給される暗号化コンテンツが復号処理され、データがトランスポートストリームである場合は、復号データがバス110を介して、TS処理手段300に出力され、TS処理が不要の場合は入出力1/F120に供給される。

【0067】TS処理手段300は、ステップS43において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力1/F120に供給する。入出力1/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0068】さらに、データは入出力1/F120に供給され、ステップS34において、入出力1/F120はデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0069】なお、入出力1/F120は、ステップS34で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0070】記録媒体200に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0071】即ち、ステップS41、S42、S43において、図4(A)のステップS31、S32、S33における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0072】MPEGコーデック130では、ステップS44において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力1/F140に供給される。入出力1/F140は、ステップS44において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S45)して、アナログコンテンツとする。そして、ステップS46に進み、入出力1/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0073】[トランスポートストリーム] 次に、図5を用いて、トランスポートストリームデータを処理する場合における記録媒体上のデータフォーマットを説明する。記録媒体上のデータの読み書きの最小単位をブロック(block)という名前と呼ぶ。1ブロックは、192×X(エクス)バイト(例えばX=32)の大きさとな

っている。

【0074】例えばMPEG2のTS(トランスポート・ストリーム)パケット(188バイト)にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとする。ATSは24乃至32ビットの着信時刻を示すデータであり、Arrival Time Stamp(着信時刻スタンプ)の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック(セクタ)には、ATSを付加したTS(トランスポート・ストリーム)パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック(セクタ)のデータを暗号化するブロックキーを生成する。

【0075】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0076】なお、図5に示すブロック・シード(Block Seed)は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなく、図中段に示すようにコピー制限情報(CCI: Copy Control Information)も付加する構成が可能である。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることが出来る。

【0077】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm(たとえば、m=8または16)バイトは暗号化されずに平文(Unencrypted data)のまま記録され、残りのデータ(m+1バイト以降)が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長(Encrypted data)に制約が発生するためである。なお、もし、暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、m=4として、ブロックシード以外の部分をすべて暗号化してもよい。

【0078】[TS処理手段における処理] ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0079】すなわち、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリー

ムの中から1つまたは幾つかのTVプログラム(コンテンツ)を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる(図7(a)参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはMPEG2システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるTSTD(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【0080】トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをDVD等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すATSを付加して記録する。

【0081】図6に、デジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図1においては、入出力I/F120を介して、あるいは入出力I/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

【0082】トランスポートストリームは、ビットストリームパーサ(parser)602に入力される。ビットストリームパーサ602は、入力トランスポートストリームの中からPCR(Program Clock Reference)パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、トランスポートパケットが受信側に到着する時刻を27MHzの精度で表す。

【0083】そして、27MHzPLL603において、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック(Lock)させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード(Block seed)付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付加する。

【0084】ATSが付加されたトランスポートパケットは、スミージングバッファ606を通して、端子60

7から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、記録媒体I/F210(図1)を介してストレージメディアである記録媒体200に記録される。

【0085】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7(a)は、ある特定プログラム(コンテンツ)を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7(a)に示すように不規則なタイミングで現れる。

【0086】図7(b)は、ブロック・シード(Block Seed)付加回路605の出力を示す。ブロック・シード(Block Seed)付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すATSを含むブロック・シード(Block Seed)を付加して、ソースパケットを出力する。図7(c)は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7(c)に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0087】図8は、記録媒体200に記録されたトランスポートストリームを再生する場合のTS処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたATS付きのトランスポートパケットが、ブロック・シード(Block seed)分離回路801へ入力され、ATSとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

【0088】なお、再生の開始時において、一番最初のATSが初期値として、タイミング発生回路804にセットされる。比較器803は、ATSとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とATSが等しくなった時、出力制御回路802は、そのトランスポートパケットをMPEGコーデック130またはデジタル入出力I/F120へ出力する。

【0089】図9は、入力AV信号を記録再生器100のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0090】MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPE

Gビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報である。

【0091】端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ905へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0092】多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG2で規定されている仮想的なデコーダモデルであるT-S-TDを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【0093】パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0094】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0095】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0096】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0097】多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0098】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体200へ格納される。

【0099】記録媒体200へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体200に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0100】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンタが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリカウンタである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0101】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報



(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

【0102】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な情報を利用することが可能である。

【0103】[キー配信構成としてのツリー(木)構造について]次に、図1に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なキー、例えばメディアキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図11に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

【0104】各デバイス0~15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR~K111をノードキーとする。

【0105】図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー: K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0106】また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタ

イプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図11に示すキー配布構成が適用されている。

【0107】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0108】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0109】このツリー構成において、図11から明らかのように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00、Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00、Kmaster)を解いてマスターキー: Kmasterを得ることが可能となる。なお、Enc(Ka、Kb)はKbをKaによって暗号化したデータであることを示す。

【0110】また、ある時点tにおいて、デバイス3の所有する鍵: K0011、K001、K00、K0、KRが攻撃者(ハッカー)により解析されて露呈したことが発

覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation)：tの更新キーであることを示す。

【0111】更新キーの配布処理について説明する。キーの更新は、例えば、図12(A)に示す有効化キーブロック(EKB：Enabling Key Block)と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

【0112】図12(A)に示す有効化キーブロック(EKB)には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図12の例は、図11に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図11から明らかなように、デバイス0, デバイス1は、更新ノードキーとしてK(t)00, K(t)0, K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001, K(t)00, K(t)0, K(t)Rが必要である。

【0113】図12(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図12(A)の下から2段目の暗号化キーEnc(K(t)001, K(t)00)を復号可能となり、更新ノードキーK(t)00を得ることができる。以下順次、図12(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図12(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。一方、デバイス0, 1は、ノードキーK000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)Rである。デバイス0, 1は、図12(A)の上から3段目の暗号化キーEnc(K000, K(t)00)を復号しK(t)00、を取得し、以下、図12(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図12(A)の上から1段目の暗号化キーEnc(K(t)

0, K(t)R)を復号しK(t)Rを得る。このようにして、デバイス0, 1, 2は更新した鍵K(t)Rを得ることができる。なお、図12(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0114】図11に示すツリー構造の上位段のノードキー：K(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図12(B)の有効化キーブロック(EKB：Enabling Key Block)を用いることで、更新ノードキーK(t)00をデバイス0, 1, 2に配布することができる。

【0115】図12(B)に示すEKBは、例えば特定のグループにおいて共有する新たなマスターキー、あるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図11に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のマスターキーK(t)masterが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新マスターキー：K(t)masterを暗号化したデータEnc(K(t), K(t)master)を図12(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

【0116】すなわち、デバイス0, 1, 2はEKBを処理して得たK(t)00を用いて上記暗号文を復号すれば、t時点でのマスターキー：K(t)masterやメディアキー：K(t)mediaを得ることが可能になる。

【0117】[EKBを使用したメディアキーの取得] 図13に、本出願人の先の特許出願である特願平2000-105328で提案したt時点でのメディアキーK(t)mediaを得る処理例として、K(t)00を用いて新たな共通のメディアキーK(t)mediaを暗号化したデータEnc(K(t)00, K(t)media)と図12(B)に示すEKBとを記録媒体を介して受領したデバイス2の処理を示す。

【0118】図11に示すように、ある記録再生システムには、点線で囲まれた、デバイス0, 1, 2, 3の4つの装置が含まれるとする。図13は、デバイス3がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置(デバイス2)が記録媒体上のコンテンツを暗号化もしくは復号するために必要なメディアキーを、記録媒体に格納されているEKB(Enabling Key Block)と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

【0119】デバイス2のメモリには、自分にのみ割り当てられたリーフキーK\_0010と、それから木のルートまでの各ノード001, 00, 0, Rのノードキー



(それぞれ、 $K_{001}$ ,  $K_{00}$ ,  $K_0$ ,  $K_R$ ) が安全に格納されている。デバイス2は、図13の記録媒体に格納されているEKBのうち、インデックス(index)が0010の暗号文を自分の持つリーフキー $K(t)_{001}$ で復号してノード001のノードキー $K(t)_{001}$ を計算し、次にそれを用いてインデックス(index)が001の暗号文を復号してノード00のノードキー $K(t)_{00}$ を計算し、最後にそれを用いて暗号文を復号してメディアキー $K(t)_{media}$ を計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

【0120】[メディアキーを用いたコンテンツ記録処理] 図14の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理および記録媒体に対する記録処理の一例について説明する。

【0121】図14に示す記録再生装置100は自身の上述したEKBに基づく算出処理によってメディアキーを取得する。

【0122】次に、記録再生装置100は例えば光ディスクである記録媒体200に識別情報としてのディスクID(Disc ID)が既に記録されているかどうかを検査する。記録されていれば、ディスクID(Disc ID)を読み出し、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID(Disc ID)を生成し、ディスクに記録する。ディスクID(Disc ID)はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0123】記録再生器100は、次にメディアキーとディスクIDを用いて、ディスク固有キー(Disc Unique Key)を生成する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、図15に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスクID(Disc ID)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する例2の方法が適用できる。

【0124】次に、記録ごとの固有鍵であるタイトルキー(Title Key)を暗号処理手段150(図1参照)においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク200に記録する。

【0125】次にディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)の組合せから、タイトル固有キー(Title Unique Key)を生成する。

【0126】このタイトル固有キー(Title Unique Key)生成の具体的な方法は、図16に示すように、ブロック暗号関数を用いてディスク固有キーを鍵としてタイトルキーを暗号化して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー(Title Unique Key)として使用する例2の方法が適用できる。

【0127】なお、上記の説明では、メディアキーとディスクID(Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)からタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてメディアキーとディスクID(Disc ID)とタイトルキー(Title Key)から直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、メディアキー(Master Key)とディスクID(Disc ID)からタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

【0128】さらに、図14を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第1~4バイトが分離されて出力されるブロックシード(Block Seed)と、先に生成したタイトル固有キー(Title Unique Key)とから、そのブロックのデータを暗号化する鍵であるブロック・キー(Block Key)が生成される。

【0129】ブロック・キー(Block Key)の生成方法の例を図17に示す。図17では、いずれも32ビットのブロック・シード(Block Seed)と、64ビットのタイトル固有キー(Title Unique Key)とから、64ビットのブロックキー(Block Key)を生成する例を2つ示している。

【0130】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー(Title Unique Key)をこの暗号関数の鍵とし、ブロックシード(Block Seed)と32ビットの定数(コンスタント)を連結した値を入力して暗号化した結果をブロックキー(Block Key)としている。

【0131】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー(Title Unique Key)とブロックシード(Block Seed)を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー(Block Key)としている。

【0132】なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとメディアキーとディスクID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) を用いてブロックキー (Block Key) を生成してもよい。

【0133】ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図14の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第1~mバイト (たとえばm=8バイト) は分離 (セクタ1608) されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化する。なお、暗号化されないmバイト中にはブロック・シードとしての第1~4バイトも含まれる。セクタにより分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) を用いることができる。

【0134】以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロック・シード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

【0135】次に、記録した暗号化コンテンツデータに対して、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵 (署名生成鍵) を用いてデジタル署名を計算し、これを自身の公開鍵証明書およびコンテンツデータと共に記録媒体に記録する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で規格制定中のECDSA (Elliptic Curve Digital Signature Algorithm) を用いることができる。図18にコンテンツの記録処理の概要を説明するフローチャートを示す。

【0136】まず、記録再生装置はステップS101において記録対象コンテンツの暗号化処理を実行する。コンテンツ暗号化は、図14を用いて説明したように、ブロックキーを用いたブロックデータの暗号化処理として実行される。

【0137】さらに、ステップS102において、記録再生装置は自身に割り当てられた公開鍵暗号系の秘密鍵 (署名生成鍵) を用いて暗号化コンテンツに対するデジタル署名を計算する。デジタル署名の生成方法としては、たとえば、IEEE P1363 で規格制定中のECDSA (Elliptic Curve Digital Signature Algorithm) が適用可能である。

【0138】次に、ステップS103において、記録再生装置は生成したデジタル署名と公開鍵証明書を記録コ

ンテンツに対応付けて記録媒体に記録し、ステップS104において暗号化データの記録媒体に対する記録処理 (S102) を実行する。

【0139】さらに、図19に暗号化コンテンツにデジタル署名を実行して記録を実行する場合の詳細処理フローを示す。

【0140】ステップS201において、記録再生装置は前述のEKB処理 (図13参照) によってメディアキーを取得する。

【0141】S202において、記録媒体に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS203でこのディスクIDを読み出し、記録されていなければS204で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S205では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法 (図15参照) などを適用することで求める。

【0142】次にS206に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、生成したタイトルキーをディスク (記録媒体) に記録する。次にS207で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成 (図16参照) する。

【0143】S208では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S209で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S210で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS211に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0144】次に、暗号処理手段150は、S212で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS207で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成 (図17参照) する。

【0145】S213では、ブロックキーを用いてS211で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0146】S214で、記録ブロックが第1ブロックであるか否かを判定し、第1ブロックである場合は、S215においてブロックデータをデジタル署名対象データとして、デジタル署名を生成し、公開鍵証明書とともに記録媒体に記録する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のE C-D S A (Elliptic Curve Digital Signature Algorithm)を適用する。

【0147】S216で、暗号化したブロックデータを記録媒体に記録する。S217で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS208に戻って残りのデータの処理を実行する。

【0148】以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツのブロックデータに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【0149】なお、記録媒体に格納されるコンテンツ、タイトルキー、デジタル署名、公開鍵証明書、その他コンテンツ関連データはそれぞれの対応が識別可能な構成をもって記録される。例えば管理データをテーブルとして記録媒体に記録することによって対応付けが可能である。図20に記録コンテンツに関する対応データのアドレスデータをテーブルとして記録する場合のテーブル構成例を示す。

【0150】図20に示すように、各コンテンツはコンテンツ関連データとともに、ファイルとして管理され、コンテンツデータのアドレス、タイトルキーのアドレス、デジタル署名のアドレス、公開鍵証明書のアドレス、その他ファイル情報について記録されたテーブルが生成され記録媒体に格納される。

【0151】次に、記録媒体に暗号化コンテンツを記録する際に、暗号化コンテンツに署名を実行するのではなく、コンテンツに対応して生成されるタイトルキーにデジタル署名を実行してコンテンツ記録を実行する処理について、図21のフローを用いて説明する。

【0152】ステップS301において、記録再生装置は前述のE K B 処理(図13参照)によってメディアキーを取得する。

【0153】S302において、記録媒体に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS303でこのディスクIDを読み出し、記録されていなければS304で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S305では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数S H A-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法(図15参照)などを適用することで求める。

【0154】次にS306に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、生成したタイトルキーに対するデジタル署名を実行する。デジタル署名の生成処理は例えばIEEE P1363で規格制定中のE C-D S A (Elliptic Curve Digital Signature Algorithm)を適用する。さらに、生成したタイトルキー、デジタル署名、および公開鍵証明書を記録媒体(ディスク)に格納する。

【0155】次にS307で、上記のディスク固有キーとタイトルキーとから、タイトル固有キーを生成(図16参照)する。

【0156】S308では、記録再生装置は記録すべきコンテンツデータの被暗号化データをT S パケットの形で受信する。S309で、T S 処理手段300は、各T S パケットを受信した時刻情報であるA T S を付加する。あるいはコピー制御情報C C I とA T S、さらに他の情報を組み合わせた値を付加する。次に、S310で、A T S を付加したT S パケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS311に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0157】次に、暗号処理手段150は、S312で、ブロックデータの先頭の32ビット(A T S を含むブロック・シード)とS307で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成(図17参照)する。

【0158】S313では、ブロックキーを用いてS311で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるD E S (Data Encryption Standard) が適用される。

【0159】S314で、暗号化したブロックデータを記録媒体に記録する。S315で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS308に戻って残りのデータの処理を実行する。

【0160】以上の処理により、コンテンツが暗号化されて記録媒体に記録され、さらに、暗号化コンテンツに対応するタイトルキーに対するデジタル署名、および公開鍵証明書が記録媒体に記録されることになる。

【0161】上記の例ではタイトルキーにデジタル署名を施したが、タイトルキーとディスクIDに対してデジタル署名を施してもよい。このようにすることにより、そのデータがそのディスクに記録されたということを明確にでき、そのデータが他のディスクにコピーされたものは不正なコピーであるという判断が容易に行える。

【0162】[メディアキーを用いたコンテンツ再生処

理] 次に、記録媒体に格納された暗号化コンテンツデータの復号および再生処理を図22以下を用いて説明する。

【0163】再生処理においては、再生装置はまず、再生するコンテンツデータと共に記録されている記録装置の公開鍵証明書とデジタル署名を読み出し、これらの正当性を確認する。

【0164】すなわち、再生装置が保持している、信頼できるセンタの公開鍵（署名検証鍵）を用いて公開鍵証明書の正当性を検査し、これに成功すれば、公開鍵証明書に含まれている、記録装置の公開鍵（署名検証鍵）を用いて記録装置が作成して記録したデジタル署名を検査する。デジタル署名の検査方法としては、たとえば、前述のECDSAを用いることができる。

【0165】次に、再生装置は、記録されている公開鍵証明書から記録装置の識別情報（ID）を読み出し、これとリボケーション情報からこの記録装置がシステムからリボーク（排除）されていないことを確認する。

【0166】（リボケーションリストを用いたリボーク検査）リボケーション情報としては、たとえば図23に示すリボケーションリストを用いることができる。リボケーションリストは図に示すようにリボーク（排除）する機器のIDを併記したデータと、リストのバージョンナンバーに対してセンタがデジタル署名を施したものである。このリボケーションリストは、たとえば、1）製造される機器（記録再生装置）のメモリに記憶させる。さらに、2）コンテンツデータと一緒にネットワークや記録媒体を介して流通させる。などの方法で、システム内を流通させることにより、再生処理時に再生装置がより新しいリボケーション情報を得られるようにしておく。

【0167】また、リボケーションリストを使用する際には、リストが偽造、改ざんされたものでないことを検査するために、リボケーションリスト内に格納されたセンタの署名の検証処理を実行する。署名の検証処理は、公開鍵証明書の署名検証と同様、予め機器（記録再生装置）が持っているセンタの公開鍵（署名検証鍵）を用いて検査することが可能である。

【0168】（EKBを利用したリボーク検査）また、リボケーション情報を図23に示すようなリストとして各機器に配布する構成をとらず、リボークされているかをEKBを使用して判別する構成としてもよい。たとえば図11に示したツリー状に機器が配置されたシステムにおいて、図12の（A）例1に示すEKBが記録媒体に格納されていたとする。このとき、各機器は、EKBのインデックスを逐次みていくと、EKBで更新されるノードキーをツリー状に表したものが図24の太線のようになることが理解できる。

【0169】そして、更新されたノードキーを得られるのは、太線で示したツリーのリーフ（葉）の下に位置す

る機器だけ、つまり、デバイス0, 1, 2だけであることが理解できる。そして、それ以外の機器はシステムからリボークされていると判断することができ、これらのIDを持った機器が記録したコンテンツデータの再生を禁止する処理を、再生処理の実行時に実行することによりリボーク機器による記録コンテンツの再配布を停止することが可能となる。なお、この例では、図11におけるリーフの位置と、デバイスのIDが対応していることを前提としている。すなわち、有効化キープブロック（EKB）のインデックスのトレース処理を前記IDに基づいて実行することでリボークの有無を判別する。

【0170】トレース処理によるリボーク検査について詳細に説明する。まず、図25に有効化キープブロック（EKB）のフォーマット例を示す。バージョン1001は、有効化キープブロック（EKB）のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプス1002は、有効化キープブロック（EKB）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ1003は、有効化キープブロック（EKB）中のデータ部の位置を示すポインタであり、タグポインタ1004はタグ部の位置、署名ポインタ1005は署名の位置を示すポインタである。

【0171】データ部1006は、例えば更新するノードキーを暗号化したデータを格納する。例えば図13に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0172】タグ部1007は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図26を用いて説明する。図26では、データとして先に図12（A）で説明した有効化キープブロック（EKB）を送付する例を示している。この時のデータは、図26の表（b）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK（t）Rが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータEnc（K（t）0, K（t）R）は、図26の（a）に示す階層ツリーに示す位置にある。ここで、次のデータは、Enc（K（t）00, K（t）0）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左（L）タグ, 右（R）タグ}として設定される。最上段のデータEnc（K（t）0, K（t）R）の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図26（c）に示すデータ列、およびタグ列が構成される。

【0173】タグは、データEnc（Kxxx, Kyyy）がツリー構造のどこに位置しているのかを示すため

に設定されるキー配置識別タグである。データ部に格納されるキーデータ  $Enc(K_{xxx}, K_{yyy}) \dots$  は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図12で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0:  $Enc(K(t)0, K(t)root)$

00:  $Enc(K(t)00, K(t)0)$

000:  $Enc(K(t)000, K(t)00)$

... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0174】図25に戻って、EKBフォーマットについてさらに説明する。署名(Signature)は、有効化キーブロック(EKB)を発行したEKB発行局、例えば認証局、鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック(EKB)を発行者が発行した有効化キーブロック(EKB)であることを確認する。

【0175】図26に関する説明から理解されるようにEKB内に格納されたタグは自ノードの左及び右のノードの鍵データの有無を0, 1で示している。すなわちデータがある場合は0、データがない場合を1として設定される。リーフIDに基づくEKBの追跡処理、すなわち辿り方は、このような条件設定に基づくタグを用いて行われる。

【0176】リーフIDに基づくEKBの追跡(辿り方)について、図27を用いて説明する。図27(a)に示すようにリーフキーK1001を持つデバイスをリボークデバイス[1001]とする。このとき、EKBは、図27(b)のような暗号化キーとタグの構成を持つ。図27(b)のEKBは、図27(a)の1つのデバイス[1001]をリボークするために、KR, K1, K10, K100を更新したEKBとなる。

【0177】このEKBを処理することにより、リボークデバイス[1001]以外のリーフはすべて更新されたルートキーK(t)Rを取得できる。すなわち、ノードキーK0の下位につらなるリーフは、更新されていないノードキーK0をデバイス内に保持しているので、 $Enc(K0, K(t)R)$ をK0によって復号することで更新ルートキーK(t)Rを取得可能となる。また、K11以下のリーフは更新されていないK11を用いて、 $Enc(K11, K(t)1)$ をK11によって復号することで更新ノードキーK(t)1を取得して、さ

らに、 $Enc(K(t)1, K(t)R)$ をK(t)1によって復号することで更新ルートキーを取得できる。K101の下位リーフについても復号ステップが1つ増加するのみで、同様に更新ルートキーを取得できる。

【0178】また、リボークされていないリーフキーK1000を持つデバイス[1000]は、自己のリーフキーで、 $Enc(K1000, K(t)100)$ を復号して、K(t)100を取得後、上位のノードキーを順次復号して更新ルートキーを取得できる。

【0179】リボークされたデバイス[1001]のみが、自己のリーフの一段上の更新ノードキーK(t)100をEKB処理により取得できないので、結局、更新ルートキーK(t)Rを取得することができない。

【0180】リボークされていない正当なデバイスには、図27(b)に示すデータ部と、タグを有するEKBがEKB発行局から配信され、デバイス内に格納されている。

【0181】リボーク検証を行なおうとするデバイスは、図27(a)のリボークデバイス[ID=1001]の公開鍵証明書の検証の後、公開鍵証明書からIDを取得する。このIDは[1001]であり、EKB配信ツリー構成のリーフ位置を示している。

【0182】ID[1001]を取り出したデバイスは、ID=1001のリーフに対応するデバイスが、EKBにおいて有効なリーフデバイスとして設定されているかを検証する。この検証は、すなわち、リーフ[1001]が更新されたルートキーK(t)Rを取得できるか否かを判定する処理として実行される。

【0183】例えば、非更新ノードキー(ex. 図27(a)のK0, K11など)の下位に属するリーフであれば、リボークされていないことが明らかであり、正当デバイスであると判定可能であり、更新ノードキーの下位に属するリーフである場合は、その更新ノードキーを取得可能な暗号化データがEKBに格納されているか否かによって、そのエンティティがリボークされているか否かを判定可能となる。

【0184】判定処理の一例として、EKBに格納されたタグに基づいてEKB追跡処理を行なう例を説明する。EKB追跡処理は、上位のルートキーからキー配信ツリーを辿れるか否かを判定する処理である。例えば図27のリーフ[1001]のIDである[1001]を[1]、[0]、[0]、[1]の4ビットとして、最上位ビットから順次下位ビットに従ってツリーを辿る。ビットが1であれば右側、0であれば左に進む。

【0185】図27(a)のルートから、ID[1001]の最上位ビットは1であり、右側に進む。EKB内の最初のタグは、0: {0, 0}であり、両枝にデータを有することが判定され、右側に進みK1に辿り着ける。次にK1の下位のノードに進む。ID[1001]の2番目のビットは0であり、左側に進む。K1の下位

のデータ有無を示すタグは、図27(a), (b)の2: {0, 0}であり、両枝にデータを有すると判定され、左側に進みK10に辿り着ける。さらに、ID[1001]の3番目のビットは0であり、左側に進む。K10の下位のデータ有無を示すタグは、図27(a), (b)の3: {0, 0}であり、両枝にデータを有すると判定され、左側に進みK100に辿り着ける。さらに、ID[1001]の最下位ビットは1であり、右側に進む。K100の下位のデータ有無を示すタグは、図27(a), (b)の5: {0, 1}であり、右側にはデータを持たない。従ってノード[1001]には辿りつけないことが判定され、ID[1001]のデバイスはEKBによる更新ルートキーを取得できないデバイス、すなわちリボークデバイスであると判定される。

【0186】例えば図27(a)のリーフキーK1000を有するデバイスIDは[1000]であり、上述と同様のEKB内のタグに基づくEKB追跡処理、すなわちツリーを辿る処理を実行すると、ノード[1000]に辿りつくことができるので、EKBによる更新ルートキーを取得可能なリボークされていない正当なデバイスであると判定される。

【0187】また、例えば更新されていないノードキー、例えばK0, K11などの下位のリーフにも、リーフ自体には、辿り着けないが、この場合は、更新されていない末端ノードに辿りつくことが可能である。更新されていないノードの下位のリーフは、更新されていないノードキーを用いてEKBの処理が可能であり、更新ルートキーを取得できるので正当なデバイスである。更新されていないノードキーであるか否かは、そのノードに対応するタグにより判定することが可能となる。更新されていないノードキーK0, K11, K101に対応するタグは1: {1, 1}、4: {1, 1}、6: {1, 1}となり、これらはさらに下位ノードまたはリーフが存在するが、EKB内には暗号化鍵データを持たないことを示しており、これらの下位のリーフのデバイスはリボークされていない有効な正当デバイスであると判定される。

【0188】図27に示す例は、1つのデバイスについてのみのリボーク態様であるが、図28に示すようにあるノードの下にあるすべてのリーフデバイスを一括してリボークすることも可能である。この場合のEKBのデータ(暗号化キー)、タグは図28(b)のようになる。

【0189】例えば、デバイスがリボークされたK1000に対応するリーフデバイスの公開鍵証明書からID[1000]を取得したとすると、このID[1000]に基づいてEKBのタグに基づいてツリーを辿る処理を実行する。

【0190】図28(a)のルートから、ID[1000]の最上位ビットは1であり、右側に進む。EKB内

の最初のタグ0: {0, 0}であり、両枝にデータを有することが判定され、右側に進みK1に辿り着ける。次にK1の下位のノードに進む。ID[1000]の2番目のビットは0であり、左側に進む。K1の下位のデータ有無を示すタグは、図13(a), (b)の2:

{1, 0}であり、左側にはデータを持たない。従ってノード[1000]には辿りつけない。このときの末端ノードK1に対応するタグは{1, 0}であり、下位のデータを持たない{1, 1}ではない。

【0191】タグ{1, 0}は、K1の右側の下位のノードまたはリーフにおいてのみ復号可能な更新されたK1(t)を取得するための暗号化鍵データがEKBに格納されていることを示している。

【0192】このように、リーフIDに基づいて辿り着く最終地点がノードであり、その最終ノードの対応タグが{1, 1}以外の値を持っている場合は、さらに下位の暗号化鍵データをEKB内に有することを示している。この場合は、そのIDを持つリーフデバイスはEKBの処理によって更新されたルートキーを取得することができないので、リボークされたデバイスであると判定される。

【0193】このようにして、認証処理において通信相手から取得した公開鍵証明書に格納されたリーフIDに基づいて通信相手がリボークされているか否かを判定することが可能となる。

【0194】図29にEKBを利用したリボークデバイス判定処理についての処理フローを示す。フローの各ステップについて説明する。ステップS351において、検査対象の公開鍵証明書からIDを取得する。ステップS352において、取得したIDを用いてEKBのタグに基づいて、IDの示すリーフまたはリードを目標とする追跡処理を実行する。

【0195】追跡処理は、前述の図27, 図28を用いて説明した手順で実行する。追跡処理の結果、IDの示すリーフまたはノードに辿り着くことができたか、辿りつけない場合であってもIDの示すリーフまたはノードにおいてEKB処理が可能であるか否か、すなわち更新ルートキーの取得が可能か否かを判定する(S353)。

【0196】EKB処理が可能である位置にあるIDであると判定されれば、ステップS354に進み、IDに対応するデバイスはリボークされていない正当なデバイスであると判定する。一方、EKB処理が不可能な位置にあるIDであると判定されれば、ステップS355に進み、IDに対応するデバイスはリボークされている不正なデバイスであると判定する。

【0197】なお、上述の追跡処理では、EKBのタグ部は利用しているがデータ部は利用していない。これを用いて、リボケーション情報を表す目的では、図25に示す通常のEKBではなく、データ部のないEKBを用



いることにより、それ用のEKBのサイズを小さくできる。もちろん、図25に示す、通常の、コンテンツを保護するためのEKBをリボケーション情報を表すために用いることも可能である。

【0198】上述したように、リボケーションリスト、あるいはEKBツリーのトレース処理に従ったリボーク検査により記録媒体に対してコンテンツの記録を行なった機器がリボークされているかいないかの検証を行なう。コンテンツの記録を行なった機器がリボークされていないことが検証されたことを条件として再生装置はコンテンツデータの再生処理を継続する。再生処理においては、図14を用いて説明した暗号化および記録処理と同様、メディアキーとディスクIDからディスク固有キーを生成し、ディスク固有キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体200から読み取られるブロック単位の暗号化データの復号処理を実行する。

【0199】再生処理の概要について図30のフローチャートを用いて説明する。まず、ステップS401において再生装置は、再生対象コンテンツを記録した記録媒体に格納されたコンテンツ記録装置の公開鍵証明書およびデジタル署名の検証を実行する。検証は、まず、公開鍵証明書のセンタ署名をセンタの公開鍵を用いて実行し、公開鍵証明書の正当性が確認された後、公開鍵証明書中に格納されたコンテンツ記録装置の公開鍵を取り出して、コンテンツ記録者のデジタル署名の検証を実行する。いずれの検証もOKであれば次ステップに進み、いずれかの検証がNGであれば、以降のステップ実行が禁止され再生処理はストップする。

【0200】次に、ステップS402においてコンテンツ記録装置のリボケーション検査を実行する。このリボケーション検査は、例えば予め再生装置に格納された図23に示したリボケーションリストに格納された機器IDと、公開鍵証明書内の機器IDに一致するものがあるか否かを検査することによって行われる。あるいは、前述のEKBツリー構成によるツリー探索処理を実行してもよい。ステップS402のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定されると次ステップに進み、リボークされている場合は、以降のステップ実行が禁止され再生処理はストップする。

【0201】ステップS402のリボケーション検査においてコンテンツ記録装置がリボークされていないと判定された場合、ステップS403において暗号化コンテンツの記録媒体からの読み出しが実行され、ステップS404において暗号化コンテンツの復号処理が実行されてコンテンツの再生が行われる。

【0202】このように、記録媒体に格納されたコンテ

ンツ再生処理に際し、コンテンツ記録装置のリボーク状況を判定してリボークされていない機器によって記録されたコンテンツの再生のみを実行する構成としたので、不正に記録されたコンテンツが無秩序に流通利用されることが防止される。また、リボーク判定は、公開鍵証明書に格納されたIDによって判定され、その信頼性は維持される。

【0203】次に、図31を用いて暗号化コンテンツに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【0204】ステップS501において、再生装置は記録媒体からメディアキー、ディスクIDを読み出し、ステップS502において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合(S503:No)は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【0205】署名、公開鍵証明書が存在した場合(S503:Yes)は、ステップS504において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ(認証局)の公開鍵を用いて実行される。公開鍵証明書の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0206】次に、ステップS505では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子(ID)が取り出され、リボーク検査を行なう。リボーク検査は前述の図23のリボークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリボークがないと判定されると次ステップに進み、リボークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【0207】次に、S506では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法(図15参照)などを適用することで求める。

【0208】次にS507に進みタイトルキー(Title Key)を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成(図16参照)する。

【0209】S508では、再生装置は再生すべきコンテンツデータのブロックデータを読み出す。S509で読み出しブロックが第1ブロックであるか否かを判定し、第1ブロックである場合には、ステップS510において第1ブロックに対して生成されたコンテンツ記録者(記録装置)のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書か

ら取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0210】ステップS511では、ブロックデータの先頭の32ビット（ATSを含むブロック・シード）とS507で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図17参照）する。

【0211】S512では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）が適用される。

【0212】S513で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければS508に戻って残りのデータの処理を実行する。

【0213】このように、公開鍵証明書の検証、コンテンツ記録装置のリポークの判定、暗号化コンテンツのブロックデータに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【0214】次に、図32を用いてタイトルキーに対してデジタル署名が実行された記録コンテンツの再生を実行する場合の詳細処理について説明する。

【0215】ステップS601において、再生装置は記録媒体からメディアキー、ディスクIDを読み出し、ステップS602において、タイトルキー、デジタル署名、公開鍵証明書の読み出しを実行する。署名、公開鍵証明書が存在しない場合（S603：No）は、正当な記録処理によるコンテンツではないと判定され、以降の処理の実行が停止され再生処理は終了する。

【0216】署名、公開鍵証明書が存在した場合（S603：Yes）は、ステップS604において公開鍵証明書の検証が実行される。公開鍵証明書の検証は、再生装置が保有する公開鍵証明書の発行管理を行なうセンタ（認証局）の公開鍵を用いて実行される。公開鍵証明書の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0217】次に、ステップS605では、公開鍵証明書からコンテンツ記録を実行した記録装置の識別子（ID）が取り出され、リポーク検査を行なう。リポーク検査は前述の図23のリポークリストあるいはツリー探索処理のいずれかによって実行される。コンテンツの記録装置のリポークがないと判定されると次ステップに進み、リポークありと判定されると、以降の処理の実行が停止され再生処理は終了する。

【0218】次に、ステップS606においてタイトル

キーに対して実行されたコンテンツ記録者（記録装置）のデジタル署名の検証を実行する。デジタル署名の検証は、正当性の検証された公開鍵証明書から取り出したコンテンツ記録装置の公開鍵を用いて実行される。デジタル署名の検証がOKであり正当性が確認されると次ステップに進む。正当性検証がNGの場合は、以降の処理の実行が停止され再生処理は終了する。

【0219】次に、S607では、メディアキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法（図15参照）などを適用することで求める。

【0220】次にS608に進みタイトルキー（Title Key）を読み出し、読み出したタイトルキーとディスク固有キーから、タイトル固有キーを生成（図16参照）する。

【0221】S609では、再生装置は再生すべきコンテンツデータのブロックデータを読み出す。ステップS610では、ブロックデータの先頭の32ビット（ATSを含むブロック・シード）とS608で生成したタイトル固有キーとから、そのブロックのデータを復号する鍵であるブロックキーを生成（図17参照）する。

【0222】S611では、ブロックキーを用いてブロックデータを復号する。復号アルゴリズムは、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）が適用される。

【0223】S612で、全データを読み出したかを判断する。全データを読み出していれば、再生処理を終了し、全データを読み出していなければS609に戻って残りのデータの処理を実行する。

【0224】このように、公開鍵証明書の検証、コンテンツ記録装置のリポークの判定、暗号化コンテンツのタイトルキーに対するデジタル署名の検証が順次実行され、すべての条件が満足したことに基づいてコンテンツの正当性が判定され、暗号化コンテンツの記録媒体からの復号、再生処理が実行されることになる。

【0225】上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、および記録媒体からの再生時の復号処理においては、EKBに基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、または復号処理用の鍵を生成する。

【0226】なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生装置固有のデバイスキーをEKBから取得して、これらに基づいてコンテンツデータの暗号化処理、および復号処理に用いるキーを生成する構成として



もよい。さらに、EKBから取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、および復号処理に用いるキーとして適用することも可能である。

【0227】上述のように、本発明においては、記録再生装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録するようにした。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにしているので、もし不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【0228】さらに、記録再生装置がデータを読み出す際に上記デジタル署名および公開鍵証明書の正当性を確認し、さらに記録装置がシステムからリボークされていないことを確認した後にデータを読み出す構成とした。このことにより、不正な記録装置が、不正な記録データに対してデジタル署名を記録しないような攻撃を無力なものにしていると同時に、不正な装置で記録されたデータを正当な装置で再生しないようにすることで、不正な装置のシステムからの排除をより強力に行っている。

【0229】〔記録処理におけるコピー制御〕さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0230】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0231】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1の記録再生装置の処理について、図33および図34のフローチャートを参照して説明する。

【0232】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図33

(A)のフローチャートにしたがった記録処理が行われる。図33(A)の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS701において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS702に進む。

【0233】ステップS702では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F

120が受信したコンテンツが暗号化されていない場合（例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

【0234】また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)が規定されている。EMIが00B(Bは、その前の値が2進数であることを表す)である場合は、コンテンツがコピーフリーのもの(Copy-free)であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【0235】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freeやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0236】ステップS702において、コンテンツがコピー可能でないと判定された場合、ステップS703～S705をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0237】また、ステップS702において、コンテンツがコピー可能であると判定された場合、ステップS703に進み、以下、ステップS703～S705において、図3(A)のステップS12、S13、S14における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0238】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報（例えば、DTCPにおけるembedded CCIなど）も記録される。

【0239】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0240】本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに

付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0241】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図33(B)のフローチャートにしたがった記録処理が行われる。図33(B)の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS711において、そのアナログコンテンツを受信し、ステップS712に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0242】ここで、ステップS712の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0243】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであることを表す。

【0244】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0245】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0246】ステップS712において、アナログコンテンツがコピー可能でないと判定された場合、ステップS713乃至S717をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0247】また、ステップS712において、アナログコンテンツがコピー可能であると判定された場合、ステップS713に進み、以下、ステップS713乃至S717において、図3(B)のステップS22乃至S26における処理と同様の処理が行われ、これにより、コ

ンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0248】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0249】[再生処理におけるコピー制御]次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図34(A)のフローチャートにしたがった再生処理が行われる。図34(A)の処理について説明する。まず最初に、ステップS801、S802、S803において、図4(A)のステップS31、S32、S33における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0250】入出力I/F120は、ステップS804において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0251】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMIが含まれる場合、従って、コンテンツの記録時に、DTCの規格にしたがって、EMIが記録された場合には、そのEMI(記録されたEMI(Recorded EMI))が、Copy-freelyであるときには、デジタルコンテンツは、後でコピー可能なものであると判定される。また、EMIが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【0252】なお、一般的には、記録されたEMIが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generat

ionのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0253】ステップS804において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS805に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0254】また、ステップS804において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS806に進み、入出力I/F120は、例えば、DTC Pの規格等にしがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0255】即ち、例えば、上述のように、記録されたEMIが、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0256】このため、入出力I/F120は、DTC Pの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTC Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【0257】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図34（B）のフローチャートにしたがった再生処理が行われる。図34（B）の処理について説明する。ステップS811乃至S815において、図4（B）のステップS41乃至S45における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0258】入出力I/F140は、ステップS816において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMIなどのコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0259】また、コンテンツの記録時に、例えばDTC Pの規格にしたがって、EMIまたはコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0260】また、EMIまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいて

たとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0261】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0262】ステップS816において、コンテンツが、後でコピー可能であると判定された場合、ステップS817に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0263】また、ステップS816において、コンテンツが、後でコピー可能でないと判定された場合、ステップS818に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0264】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0265】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すCGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F140は、CGMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0266】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0267】〔データ処理手段の構成〕なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化／復号LSIとして構成する

ことも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にTS処理手段300も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図35は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0268】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク2005やROM2003に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体2010に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体2010は、いわゆるパッケージソフトウェアとして提供することができる。

【0269】なお、プログラムは、上述したようなリムーバブル記録媒体2010からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部2008で受信し、内蔵するハードディスク2005にインストールすることができる。

【0270】コンピュータは、CPU (Central Processing Unit) 2002を内蔵している。CPU 2002には、バス2001を介して、入出力インタフェース2011が接続されており、CPU 2002は、入出力インタフェース2010を介して、ユーザによって、キーボードやマウス等で構成される入力部2007が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 2003に格納されているプログラムを実行する。

【0271】あるいは、CPU 2002は、ハードディスク2005に格納されているプログラム、衛星若しくはネットワークから転送され、通信部2008で受信されてハードディスク2005にインストールされたプログラム、またはドライブ2009に装着されたリムーバブル記録媒体2010から読み出されてハードディスク2005にインストールされたプログラムを、RAM (Random Access Memory) 2004にロードして実行する。

【0272】これにより、CPU 2002は、上述したフローチャートにしたがった処理、あるいは上述したブ

ロック図の構成により行われる処理を行う。そして、CPU 2002は、その処理結果を、必要に応じて、例えば、入出力インタフェース2011を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部2006から出力、あるいは、通信部2008から送信、さらには、ハードディスク2005に記録させる。

【0273】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0274】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0275】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1に示すCPU 170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU 170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0276】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0277】

【発明の効果】以上、説明したように、本発明の構成によれば情報記録装置がデータを情報記録媒体に記録する際に自身のデジタル署名および公開鍵証明書をデータと共に記録する。このことにより、情報を記録する際には、必ず、どの記録装置が記録したかという証拠もデータと共に記録するようにした。情報再生装置は、コンテンツの復号処理以前に署名および公開鍵証明書の正当性を確認し、コンテンツ記録者を特定し、公開鍵証明書、デジタル署名の改竄の無いことを確認する。本構成により、不正な記録装置による記録コンテンツの利用（再生）の効率的排除が可能となる。また、不正に記録されたデータを含む記録媒体が流通したとしても、それをどの記録装置が記録したか特定できるので、システムからの排除が行える。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例を示すブロック図である。

【図2】本発明の情報記録再生装置において適用される公開鍵証明書例を示す図である。

【図3】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図4】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図5】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図7】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図9】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図10】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報記録再生装置に対するEKB配信処理について説明するツリー構成図である。

【図12】本発明の情報記録再生装置に対するキー配布に使用されるEKBの例を示す図である。

【図13】本発明の情報記録再生装置におけるメディアキーのEKBを使用した配布例と復号処理例を示す図である。

【図14】本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

【図15】本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

【図16】本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

【図17】本発明の情報記録再生装置において適用可能なブロック・キーの生成方法を説明する図である。

【図18】本発明の情報記録再生装置におけるデータ記録処理時の暗号化処理を説明するブロック図である。

【図19】本発明の情報記録再生装置において暗号化コンテンツに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。

【図20】本発明の情報記録再生装置において記録される暗号化コンテンツと公開鍵証明書、署名等との対応を管理するテーブルの構成例を示す図である。

【図21】本発明の情報記録再生装置においてタイトルキーに対する署名を生成してデータ記録を行なう処理を説明するフロー図である。

【図22】本発明の情報記録再生装置におけるデータ再生処理時の復号処理を説明するブロック図である。

【図23】本発明の情報記録再生装置において利用されるリボケーションテーブルの構成例を示す図である。

【図24】本発明の情報記録再生装置においてEKB配信ツリーをリボークデバイスの検査に適用させる場合の処理を説明する図である。

【図25】本発明の情報記録再生装置において適用可能な有効化キーブロック(EKB)のフォーマット例を示す図である。

【図26】有効化キーブロック(EKB)のタグの構成を説明する図である。

【図27】リボークエンティティ判定のためのEKB追跡処理について説明する図(例1)である。

【図28】リボークエンティティ判定のためのEKB追跡処理について説明する図(例2)である。

【図29】リボークエンティティ判定のためのEKB追跡処理について説明するフロー図である。

【図30】本発明の情報記録再生装置において署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図31】本発明の情報記録再生装置において暗号化コンテンツに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図32】本発明の情報記録再生装置においてタイトルキーに対する署名を検証してデータ再生を行なう処理を説明するフロー図である。

【図33】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図34】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

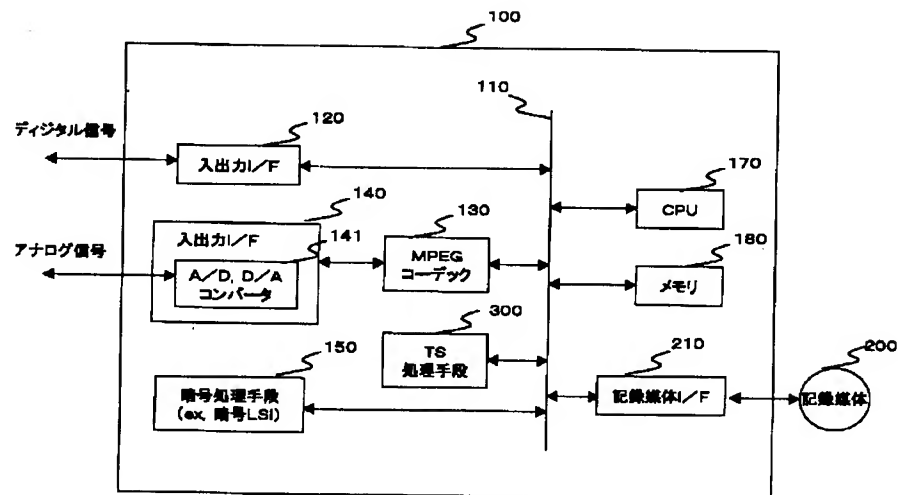
【図35】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【符号の説明】

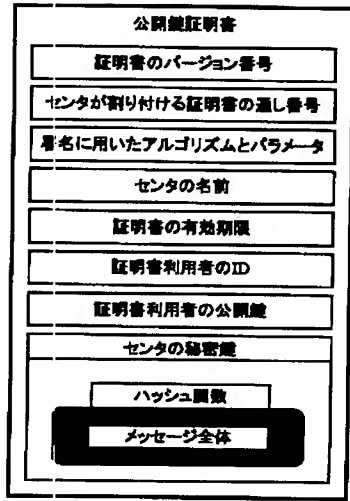
100 記録再生装置  
110 バス  
120 入出力I/F  
130 MPEGコーデック  
140 入出力I/F  
141 A/D, D/Aコンバータ  
150 暗号処理手段  
160 ROM  
170 CPU  
180 メモリ  
190 ドライブ  
200 記録媒体  
210 記録媒体I/F

300	TS処理手段	912	スムージングバッファ
600, 607	端子	976	スイッチ
602	ビットストリームパーサ	1001	バージョン
603	PLL	1002	デプス
604	タイムスタンプ発生回路	1003	データポインタ
605	ブロックシード付加回路	1004	タグポインタ
606	スムージングバッファ	1005	署名ポインタ
800, 806	端子	1006	データ部
801	ブロックシード分離回路	1007	タグ部
802	出力制御回路	1008	署名
803	比較器	2001	バス
804	タイミング発生回路	2002	CPU
805	27MHzクロック	2003	ROM
901, 904, 913	端子	2004	RAM
902	MPEGビデオエンコーダ	2005	ハードディスク
903	ビデオストリームバッファ	2006	出力部
905	MPEGオーディオエンコーダ	2007	入力部
906	オーディオストリームバッファ	2008	通信部
908	多重化スケジューラ	2009	ドライブ
909	トランスポートパケット符号化器	2010	リムーバブル記録媒体
910	到着タイムスタンプ計算手段	2011	入出力インタフェース
911	ブロックシード付加回路		

【図1】

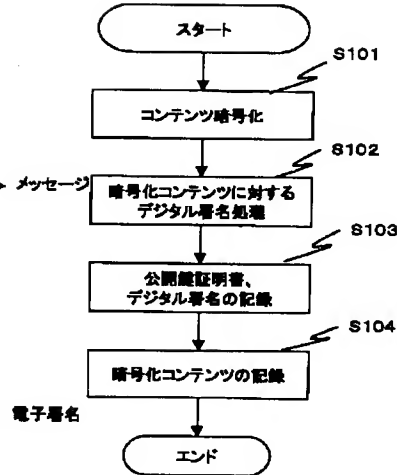


【図2】



公開鍵証明書

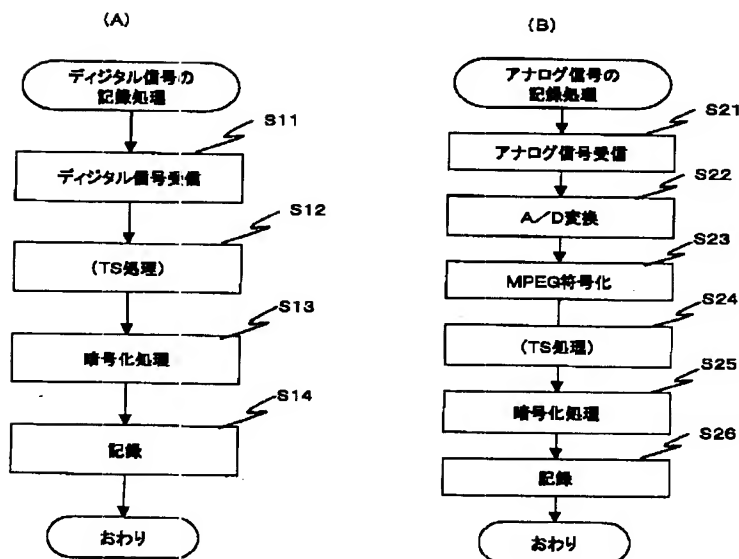
【図18】



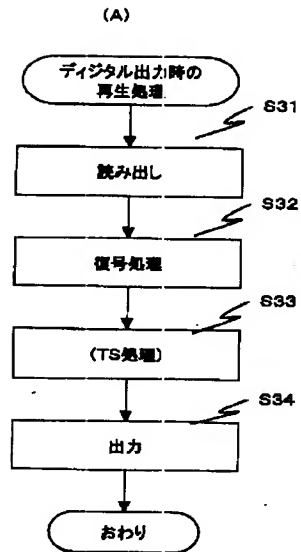
【図20】

ファイル1	コンテンツデータのアドレス
	タイトルキーのアドレス
	デジタル署名のアドレス
	公開鍵証明書のアドレス
	その他の情報
ファイル2	コンテンツデータのアドレス
	タイトルキーのアドレス
	デジタル署名のアドレス
	公開鍵証明書のアドレス
	その他の情報
⋮	⋮

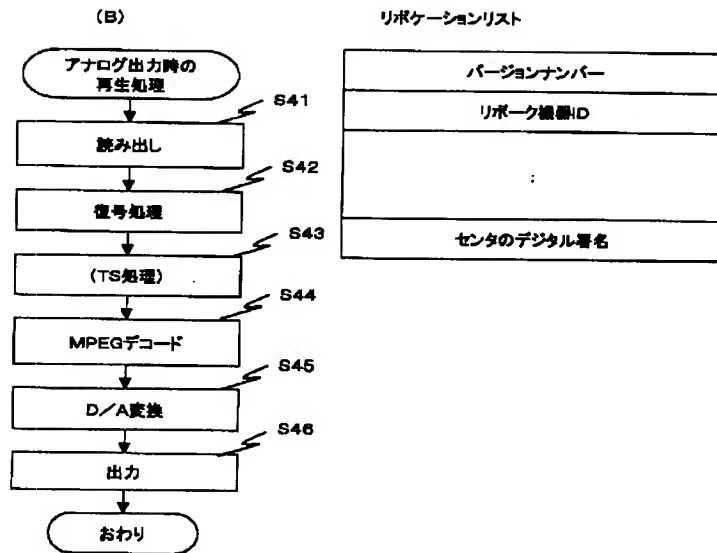
【図3】



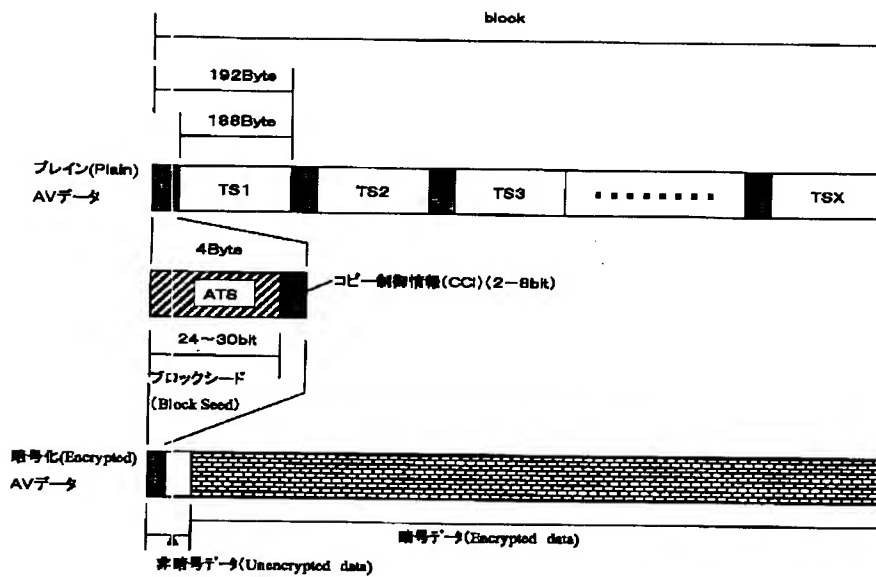
【図4】



【図23】

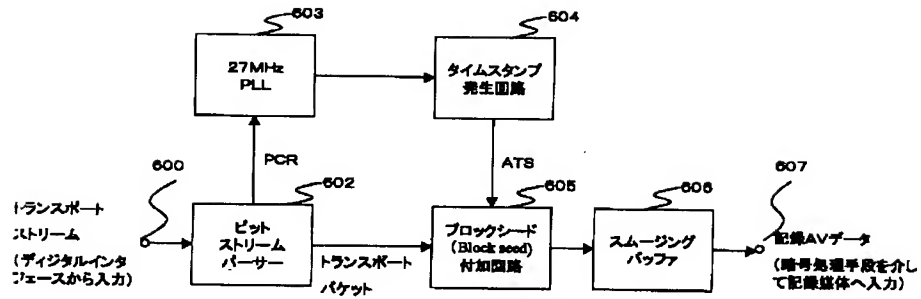


【図5】

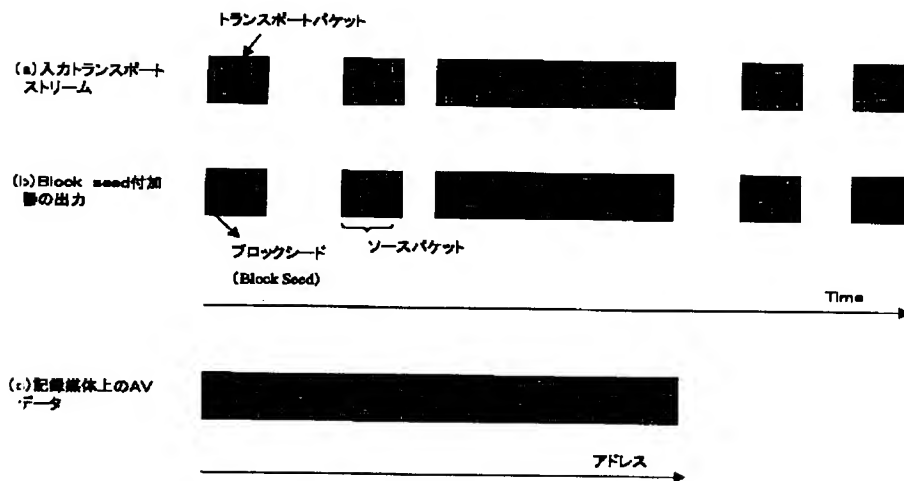




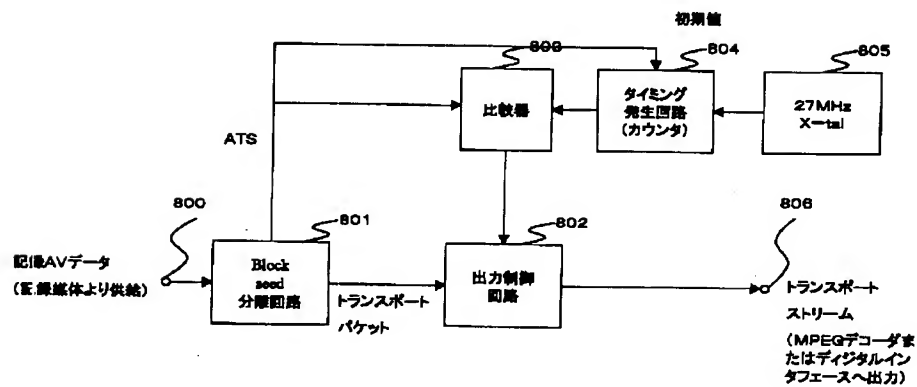
【図6】



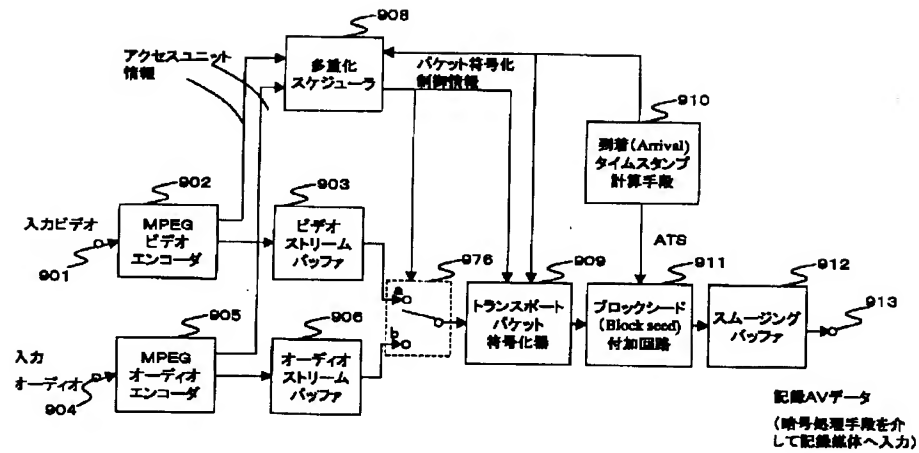
【図7】



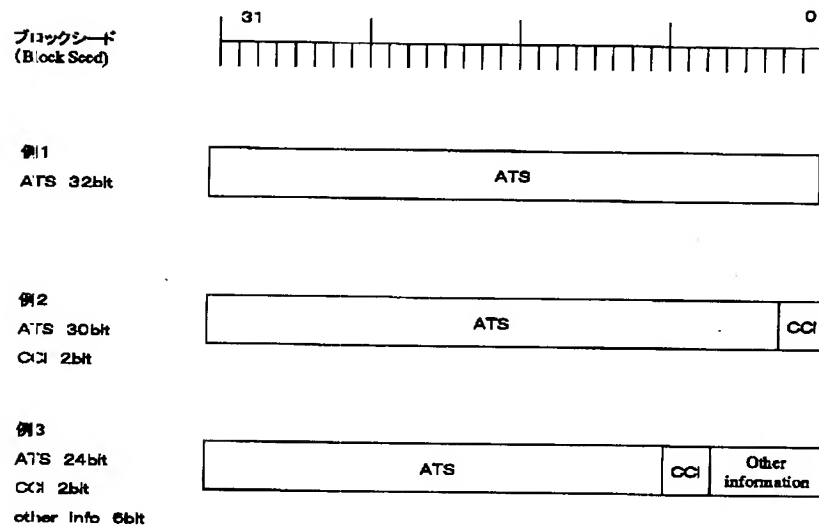
【図8】



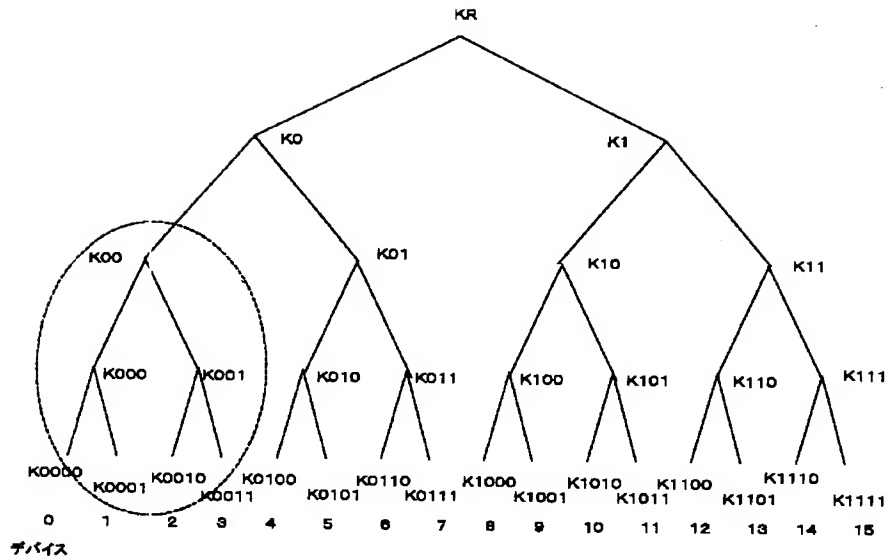
【図9】



【図10】



【図11】



【図12】

(A) 有効化キーブロック(EKB) 例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

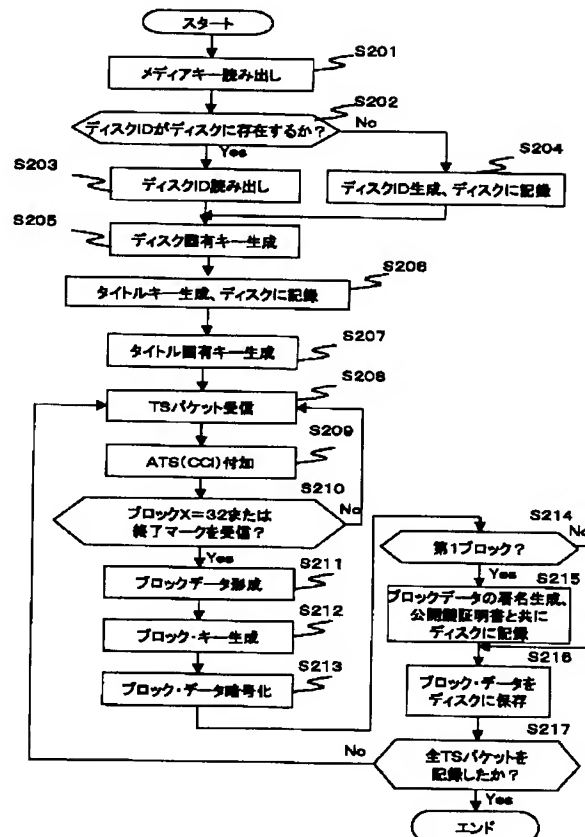
世代(Generation):t	
インデックス	暗号化キー
0	$E_{K(t)R}(K(t)R)$
00	$E_{K(t)00}(K(t)00)$
000	$E_{K(t)000}(K(t)000)$
001	$E_{K(t)001}(K(t)001)$
0010	$E_{K(t)0010}(K(t)0010)$

(B) 有効化キーブロック(EKB) 例2

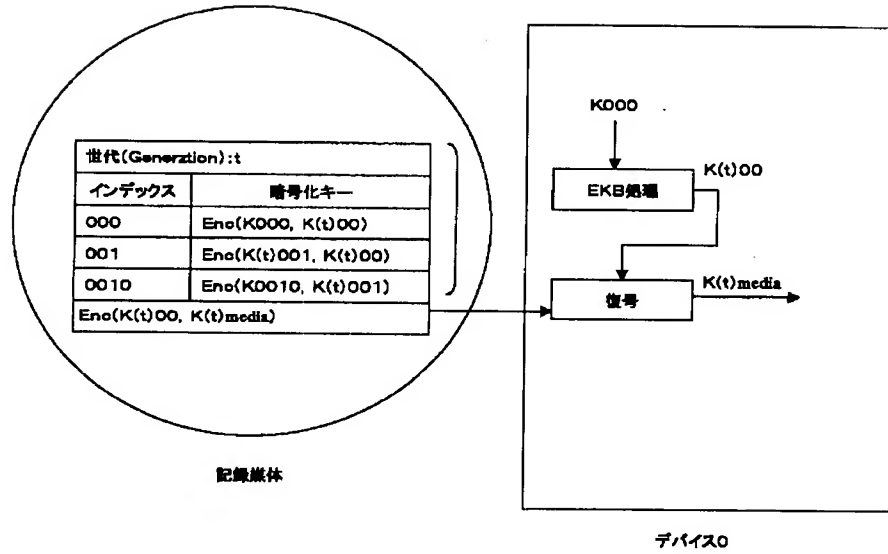
デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generation):t	
インデックス	暗号化キー
000	$E_{K(t)000}(K(t)000)$
001	$E_{K(t)001}(K(t)001)$
0010	$E_{K(t)0010}(K(t)0010)$

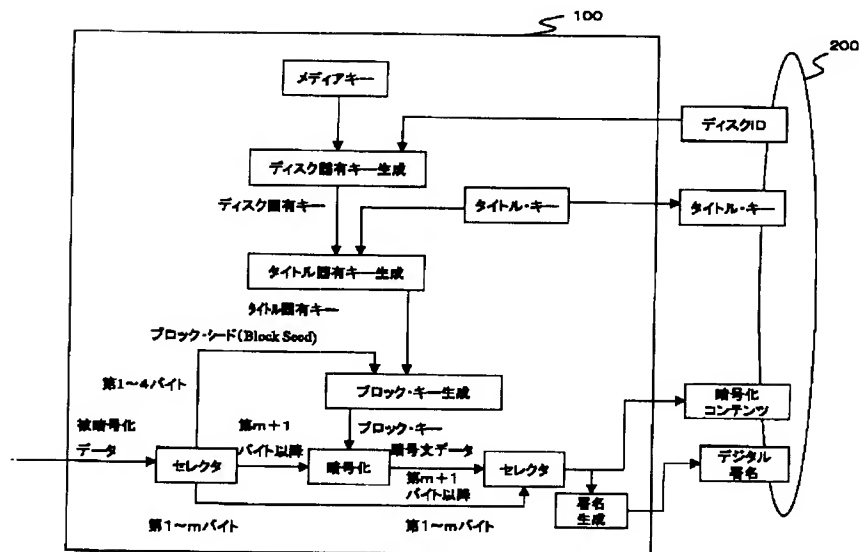
【図19】



【図13】



【図14】



【図15】

## ディスク固有キー生成例

## 入力

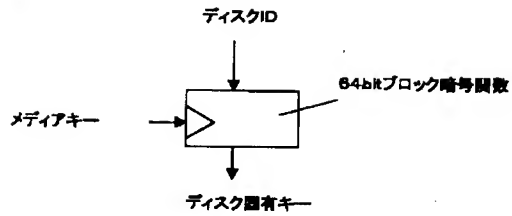
メディアキー(64bit)

ディスクID(64bit)

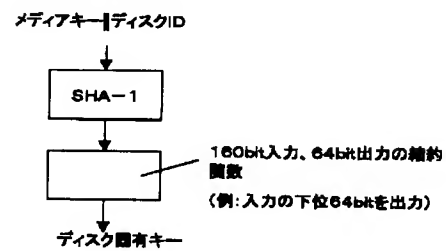
## 出力

ディスク固有キー(64bit)

## 例1



## 例2



【図16】

## タイトル固有キー生成例

## 入力

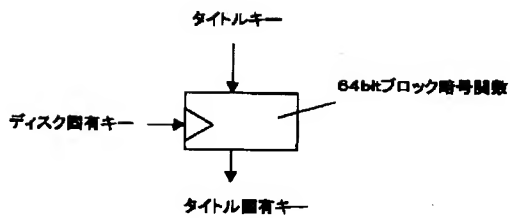
ディスク固有キー(64bit)

タイトルキー(64bit)

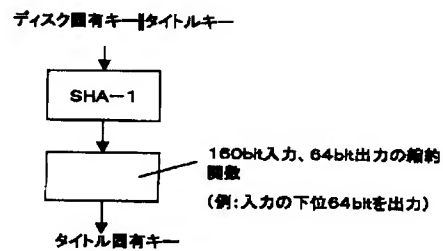
## 出力

タイトル固有キー(64bit)

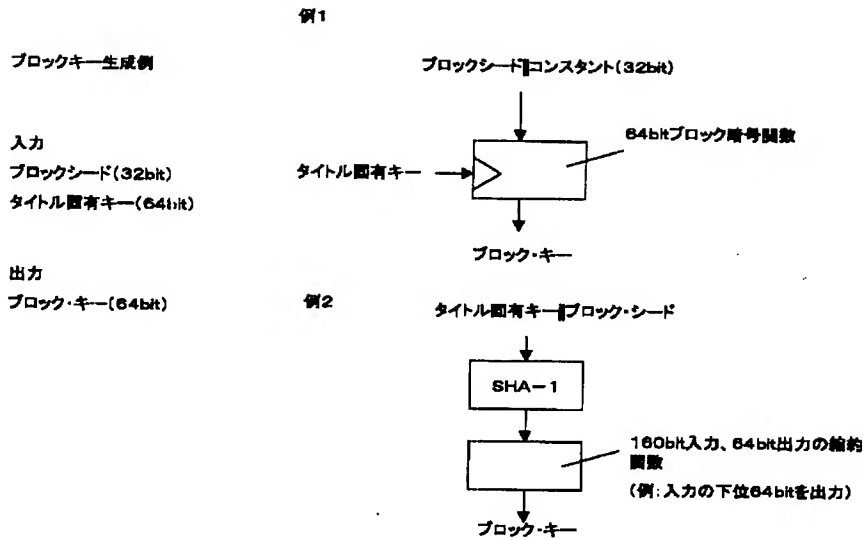
## 例1



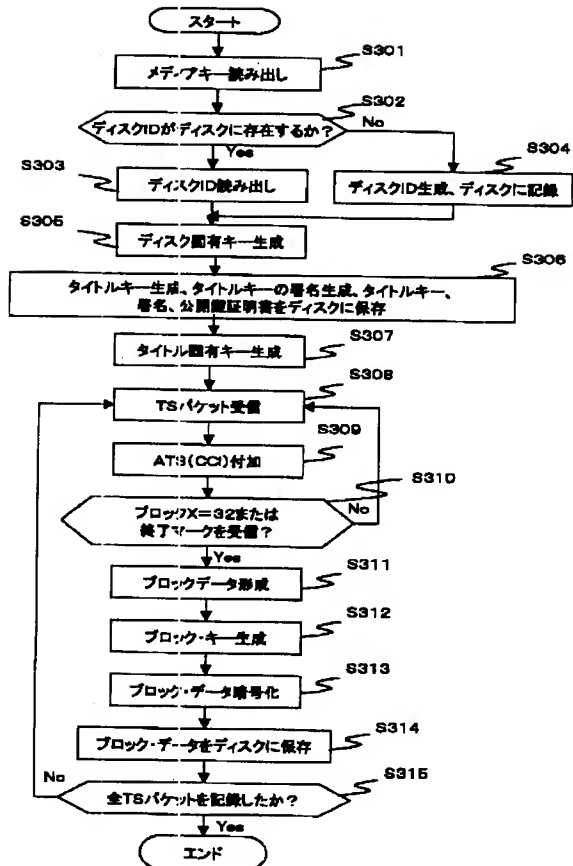
## 例2



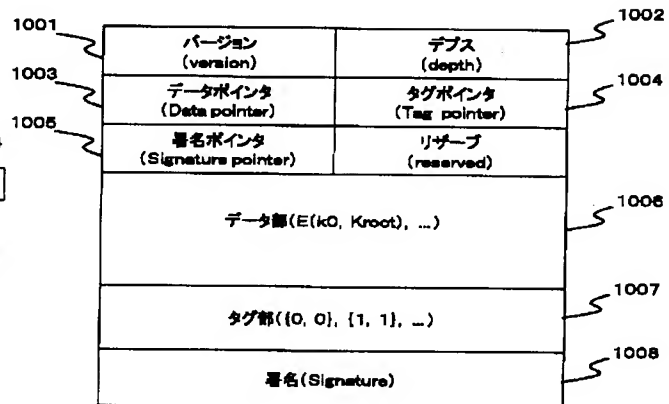
【図17】



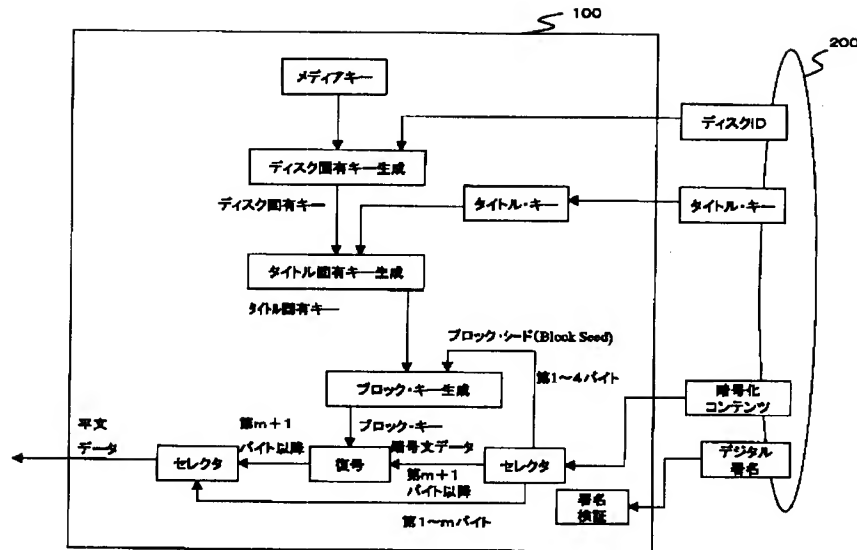
【図21】



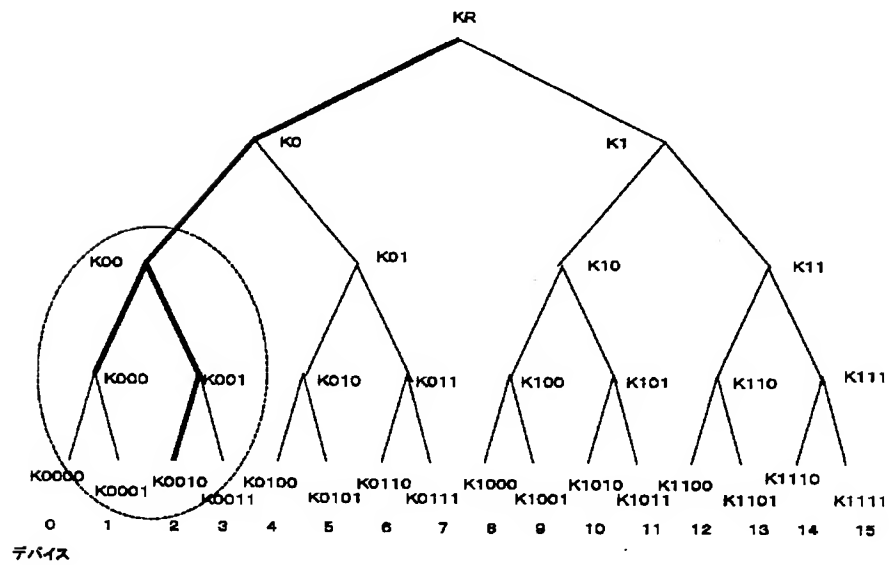
【図25】



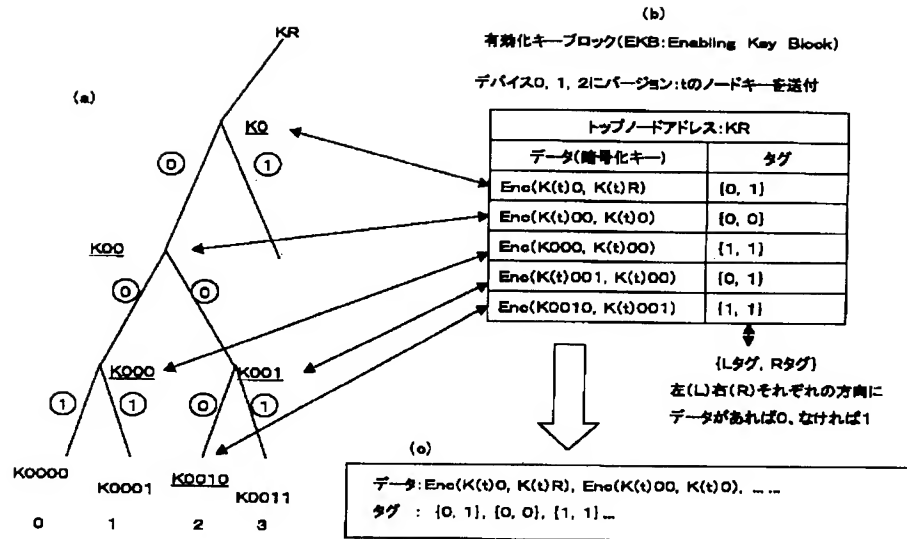
【図22】



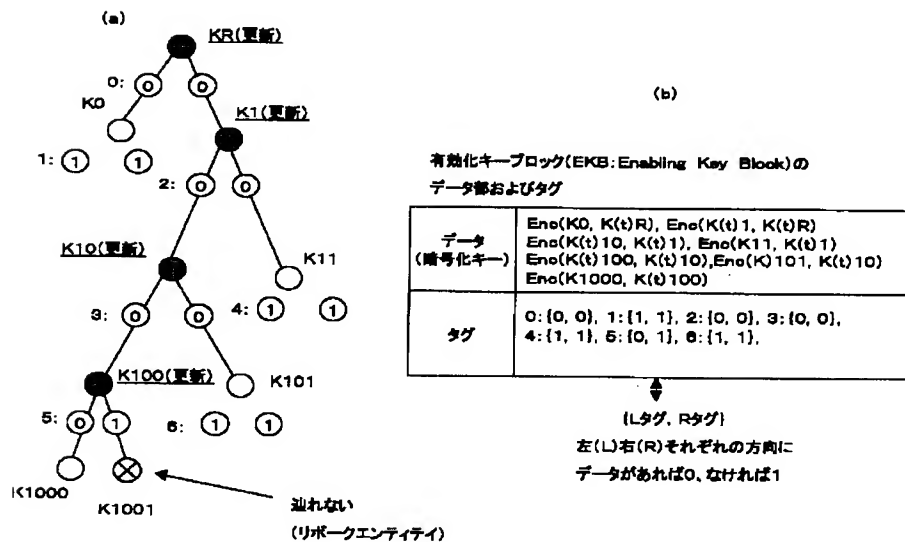
【図24】



【図26】

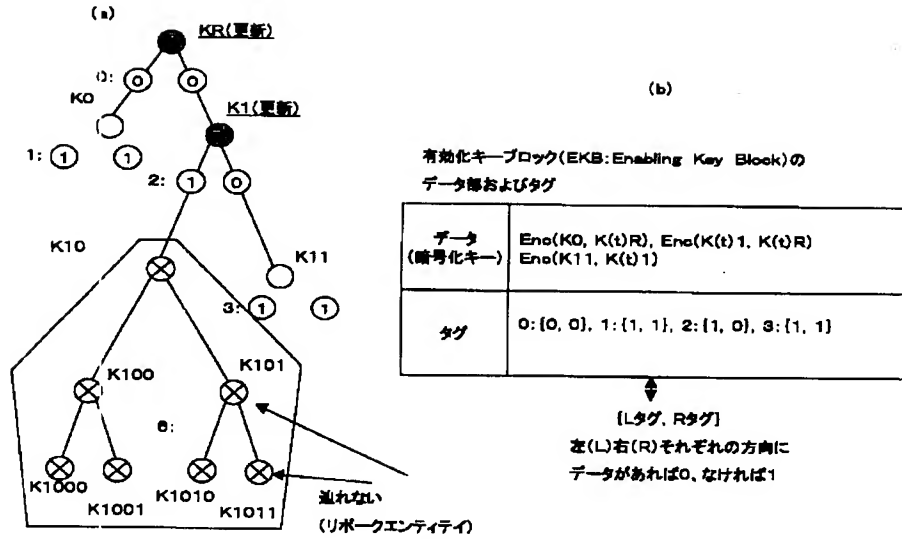


【図27】

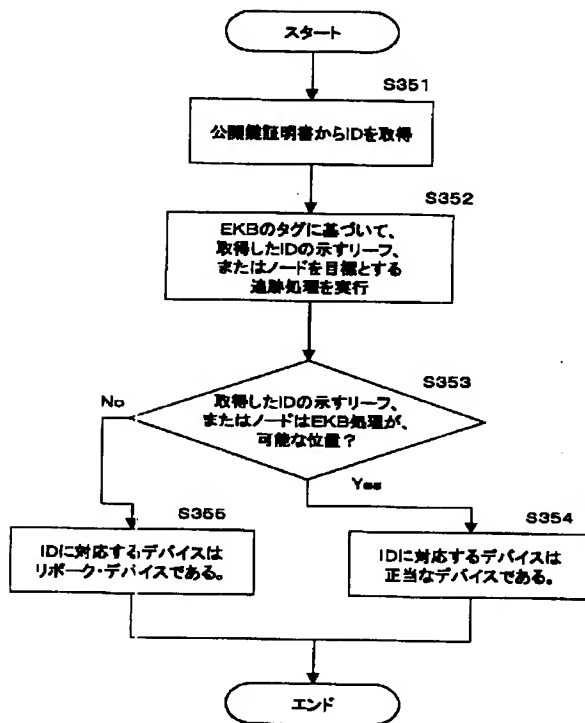




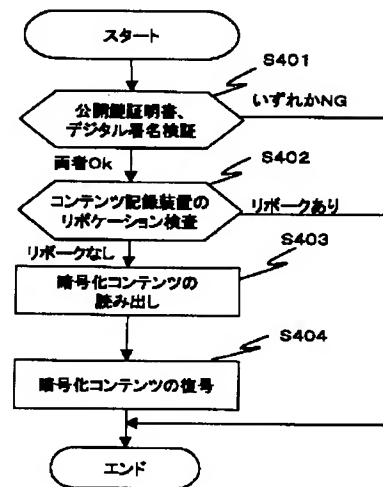
【図28】



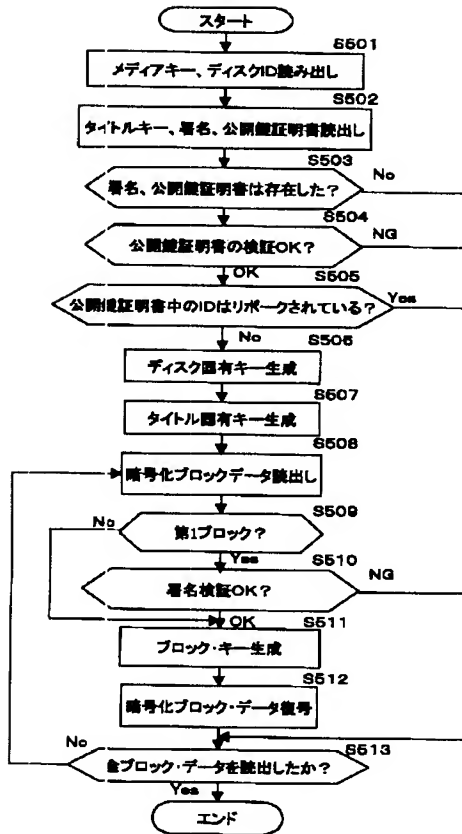
【図29】



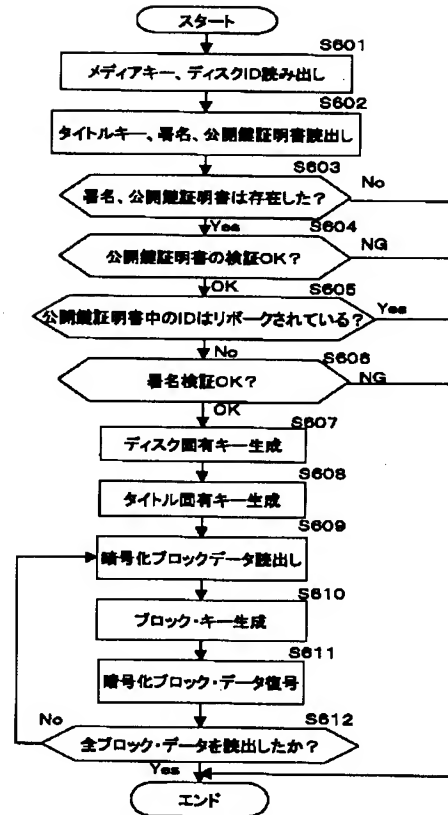
【図30】



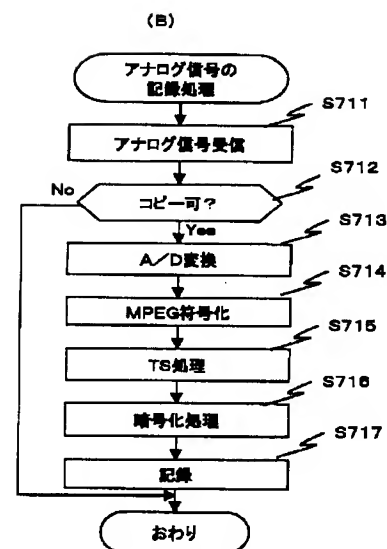
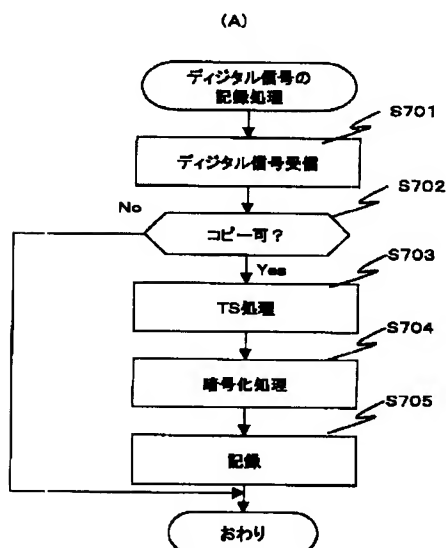
【図31】



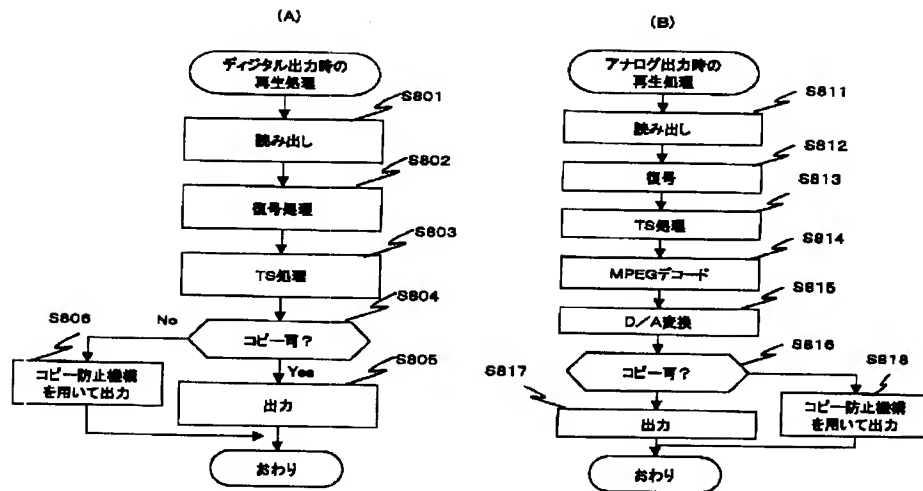
【図32】



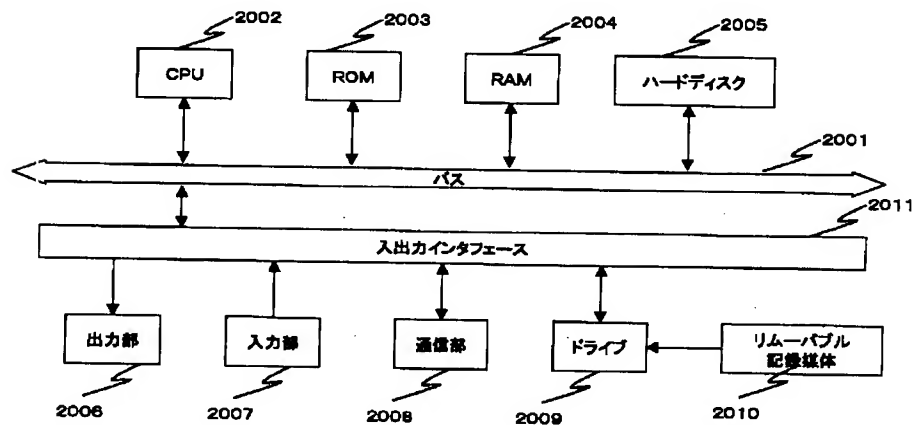
【図33】



【図34】



【図35】



【手続補正書】

【提出日】平成14年2月5日(2002.2.5)

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】図1

【補正方法】変更

【補正内容】

【図1】

